“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

网络设备安装与调试

（神码版）

张文库　周玫娜　主　编
陈韦华　周　鹏　王庆波　副主编

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

VISIT…

内 容 简 介

本书根据教育部颁发的《中等职业学校专业教学标准（试行）信息技术类（第一辑）》中的相关教学内容和要求编写。本书的编写从满足经济发展对高素质劳动者和技能型人才的需求出发，在课程结构、教学内容、教学方法等方面进行了新的探索与改革创新，以利于学生更好地掌握本课程的内容，利于学生理论知识的掌握和实际操作技能的提高。

本书以岗位工作过程来确定学习任务和目标，综合提升学生的专业能力、过程能力和职位差异能力，通过8个精彩项目，系统介绍了IP地址规划交换机的配置、路由器的配置、网络的安全配置、广域网协议配置、无线网络配置、防火墙的配置，最后通过综合实战加深对知识的掌握。

本书是计算机网络技术专业的专业核心课程教材，也可作为各类计算机网络技术培训的教材，还可以供从事网络技术相关岗位工作的人员参考学习。

本书配有教学指南、电子教案和案例素材，详见前言。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网络设备安装与调试：神码版 / 张文库，周玫娜主编. —北京：电子工业出版社，2018.8

ISBN 978-7-121-24910-5

Ⅰ. ①网… Ⅱ. ①张… ②周… Ⅲ. ①计算机网络—通信设备—设备安装—中等专业学校—教材②计算机网络—通信设备—调试方法—中等专业学校—教材 Ⅳ.①TN915.05

中国版本图书馆 CIP 数据核字（2014）第 274756 号

策划编辑：关雅莉
责任编辑：裴　杰
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：19.25　字数：492.8 千字
版　　次：2018 年 8 月第 1 版
印　　次：2018 年 8 月第 1 次印刷
定　　价：42.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254617，luomn@phei.com.cn。

编审委员会名单

主任委员：

武马群

副主任委员：

王　健　　韩立凡　　何文生

委　　员：

丁文慧　丁爱萍　于志博　马广月　马之云　马永芳　马玥桓　王　帅　王　苒

王　彬　王晓姝　王家青　王皓轩　王新萍　方　伟　方松林　孔祥华　龙天才

龙凯明　卢华东　由相宁　史宪美　史晓云　冯理明　冯雪燕　毕建伟　朱文娟

朱海波　向　华　刘　凌　刘小华　刘天真　关　莹　江永春　许昭霞　孙宏仪

苏日太夫　杜　珺　杜宏志　杜秋磊　李　飞　李　娜　李华平　李宇鹏　杨　杰

杨　怡　杨春红　吴　伦　何　琳　佘运祥　邹贵财　沈大林　宋　微　张　平

张　侨　张　玲　张士忠　张文库　张东义　张兴华　张呈江　张建文　张凌杰

张媛媛　陆　沁　陈　玲　陈　颜　陈丁君　陈天翔　陈观诚　陈佳玉　陈泓吉

陈学平　陈道斌　范铭慧　罗　丹　周　鹤　周海峰　庞　震　赵艳莉　赵晨阳

赵增敏　郝俊华　胡　尹　钟　勤　段　欣　段　标　姜全生　钱　峰　徐　宁

徐　兵　高　强　高　静　郭　荔　郭立红　郭朝勇　涂铁军　黄　彦　黄汉军

黄洪杰　崔长华　崔建成　梁　姗　彭仲昆　葛艳玲　董新春　韩雪涛　韩新洲

曾平驿　曾祥民　温　晞　谢世森　赖福生　谭建伟　戴建耘　魏茂林

序 PROLOGUE

当今是一个信息技术主宰的时代，以计算机应用为核心的信息技术已经渗透到人类活动的各个领域，彻底改变着人类传统的生产、工作、学习、交往、生活和思维方式。和语言和数学等能力一样，信息技术应用能力也已成为人们必须掌握的、最为重要的基本能力。可以说，信息技术应用能力和计算机相关专业，始终是职业教育培养多样化人才，传承技术技能，促进就业创业的重要载体和主要内容。

信息技术的发展，特别是数字媒体、互联网、移动通信等技术的普及应用，使信息技术的应用形态和领域都发生了重大的变化。第一，计算机技术的使用扩展至前所未有的程度，桌面电脑和移动终端（智能手机、平板电脑等）的普及，网络和移动通信技术的发展，使信息的获取、呈现与处理无处不在，人类社会生产、生活的诸多领域已无法脱离信息技术的支持而独立进行。第二，信息媒体处理的数字化衍生出新的信息技术应用领域，如数字影像、计算机平面设计、计算机动漫游戏和虚拟现实等。第三，信息技术与其他业务的应用有机地结合，如商业、金融、交通、物流、加工制造、工业设计、广告传媒和影视娱乐等，使之各自形成了独有的生态体系，综合信息处理、数据分析、智能控制、媒体创意和网络传播等日益成为当前信息技术的主要应用领域，并诞生了云计算、物联网、大数据和 3D 打印等指引未来信息技术应用的发展方向。

信息技术的不断推陈出新及应用领域的综合化和普及化，直接影响着技术、技能型人才的信息技术能力的培养定位，并引领着职业教育领域信息技术或计算机相关专业与课程改革、配套教材的建设，使之不断推陈出新、与时俱进。

2009 年，教育部颁布了《中等职业学校计算机应用基础大纲》。2014 年，教育部在 2010 年新修订的专业目录基础上，相继颁布了“计算机应用、数字媒体技术应用、计算机平面设计、计算机动漫与游戏制作、计算机网络技术、网站建设与管理、软件与信息服务、客户信息服务、计算机速录”等 9 个信息技术类相关专业的教学标准，确定了教学实施及核心课程内容的指导意见。本套教材就是以以上大纲和标准为依据，结合当前最新的信息技术发展趋势和企业应用案例组织开发和编写的。

本套丛书的主要特色

- **对计算机专业类相关课程的教学内容进行重新整合**

本套教材面向学生的基础应用能力，设定了系统操作、文档编辑、网络使用、数据分析、媒体处理、信息交互、外设与移动设备应用、系统维护维修、综合业务运用等内容；针对专业应用能力，根据专业和职业能力方向的不同，结合企业的具体应用业务规划了教材内容。

- **以岗位工作过程来确定学习任务和目标，综合提升学生的专业能力、过程能力和职位差异能力**

本套教材通过以工作过程为导向的教学模式和模块化的知识能力整合结构，力求实现产业需求与专业设置、职业标准与课程内容、生产过程与教学过程、职业资格证书与学历证书、终身学习与职业教育的“五对接”。从学习目标到内容的设计上，本套教材不再仅仅是专业理论内容的复制，而是经由职业岗位实践——工作过程与岗位能力分析——技能知识学习应用内化的学习实训导引和案例。借助知识的重组与技能的强化，达到企业岗位情境和教学内容要求相贯通的课程融合目标。

- **以项目教学和任务案例实训为主线**

本套教材通过项目教学，构建了工作业务的完整流程和岗位能力需求体系。项目的确定应遵循三个基本目标：核心能力的熟练程度，技术更新与延伸的再学习能力，不同业务情境应用的适应性。教材借助以校企合作为基础的实训任务，以应用能力为核心、以案例为线索，通过设立情境、任务解析、引导示范、基础练习、难点解析与知识延伸、能力提升训练和总结评价等环节，引领学习者在完成任务的过程中积累技能、学习知识，并迁移到不同业务情境的任务解决过程中，使学习者在未来可以从容面对不同应用场景的工作岗位。

当前，全国职业教育领域都在深入贯彻全国职教工作会议精神，学习领会中央领导对职业教育的重要批示，全力加快推进现代职业教育。国务院出台的《加快发展现代职业教育的决定》明确提出要“形成适应发展需求、产教深度融合、中职高职衔接、职业教育与普通教育相互沟通，体现终身教育理念，具有中国特色、世界水平的现代职业教育体系”。现代职业教育体系的建立将带来人才培养模式、教育教学方式和办学体制机制的巨大变革，这无疑给职业院校信息技术应用人才培养提出了新的目标。计算机类相关专业的教学必须要适应改革，始终把握技术发展和技术技能人才培养的最新动向，坚持产教融合、校企合作、工学结合、知行合一，为培养出更多适应产业升级转型和经济发展的高素质职业人才做出更大贡献！

前言 PREFACE

21 世纪是信息化社会，网络技术已经深入到社会生活的各个方面，深刻地影响着人们的生活和思维方式。为了适应社会发展的需要，学习和掌握计算机网络与通信方面的知识是必要的。虽然计算机网络方面的教材较多，但真正能够把理论和实践有机结合起来的教材并不多见。为了突出职业学校学生以培养技能为主的特点，“理论知识够用，强化动手能力”是本书的编写原则，希望为计算机网络实践教学提供一些参考。

“网络设备安装与调试”是网络技术专业学生必修的专业课，实践性非常强，动手实践是学好这门课程最好的方法之一。本书以知识“必需、够用”为原则，从职业岗位分析入手展开教学内容，强化学生的技能训练和职业能力，在训练中巩固所学知识。本书总结了编者多年来计算机网络工程实践及教学的经验，根据网络工程实际工作过程所需要的知识技能提炼出若干个教学项目。全书先提出学习情境，然后再提供完成该情境所必需掌握的操作技能及相关理论知识，部分项目还有知识拓展，供有余力的学生课外学习，同时安排了学习小结，本活动知识点进行了总结，在项目的最后还安排了项目考核，供课后练习。每个项目以要实现的任务为核心来组织，任务中又细分成学习活动来完成，形成了“项目—任务—活动”的结构体系，通过一个个学习活动让学生掌握相关知识和技能。每个学习活动又基本细分为“学习情境—情境分析—相关知识—步骤实现—学习小结”的结构，从工作现场需求与实践应用中引入教学项目，培养学生完成工作任务急需解决问题的技能。

本书由张文库、周玫娜担任主编并负责统稿，陈韦华、周鹏和王庆波担任副主编。教材编写分工如下：彭家龙、俸斌编写项目一，张文库编写项目二、项目三，王庆波、戴金辉编写项目四，陈韦华编写项目五、项目六，周鹏、范伟标编写项目七，周玫娜、门雅范编写项目八。

由于作者水平有限，书中难免有错误和不妥之处，恳请广大师生和读者批评指正。

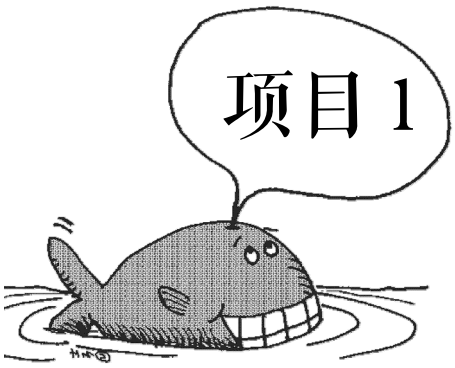
为方便教师教学，本书还配有电子教学参考资料包，包括电子教案、教学指南、素材文件、微课等，请有此需要的教师登录华信教育资源网（www.hxedu.cn）免费注册后下载。注意：请使用 IE 浏览器登录并下载。

编　者

CONTENTS | 目录

项目1　IP地址规划 …… 1
学习任务1　部门间IP地址规划 …… 1
学习任务2　合理使用IP地址 …… 7
项目2　交换机的配置 …… 14
学习任务1　交换机的基本配置 …… 15
学习活动1　交换机的管理方式 …… 15
学习活动2　交换机的基本配置 …… 22
学习活动3　交换机文件的保存和备份 …… 26
学习任务2　交换机的VLAN配置 …… 30
学习活动1　交换机的VLAN划分 …… 31
学习活动2　交换机间相同VLAN的通信 …… 37
学习活动3　利用SVI实现VLAN间路由 …… 44
学习任务3 交换机的常用技术 …… 55
学习活动1　交换机的链路聚合技术 …… 55
学习活动2　交换机的生成树技术 …… 62
学习活动3　交换机的DHCP服务 …… 70
学习活动4　交换机的VRRP服务 …… 75
学习任务4　交换机的路由配置 …… 84
学习活动1　交换机间的静态路由配置 …… 84
学习活动2　交换机间的RIP动态路由配置 …… 97
学习活动3　交换机间的OSPF路由配置 …… 109
项目3　路由器的配置 …… 124
学习任务1　路由器的基本配置 …… 124
学习活动1　路由器的简单配置 …… 125
学习活动2　路由器文件的保存和备份 …… 133
学习活动3　单臂路由的配置 …… 135
学习任务2　路由器的路由配置 …… 139
学习活动1　路由器的静态路由配置 …… 139

学习活动2　路由器的RIP动态路由配置 …… 149
学习活动3　路由器的OSPF动态路由配置 …… 159
项目4　网络的安全配置 …… 174
学习任务1　端口安全配置 …… 174
学习活动1　交换机的端口安全 …… 175
学习活动2　实现AM功能 …… 180
学习任务2　IP访问控制列表 …… 184
学习活动1　标准访问控制列表的配置 …… 184
学习活动2　扩展访问控制列表的配置 …… 193
学习活动3　命名访问控制列表的配置 …… 197
学习活动4　基于时间的访问控制列表 …… 201
学习活动5　使用ACL过滤特定病毒报文 …… 205
学习任务3　路由器IPSec VPN隧道的实现 …… 206
项目5　广域网协议配置 …… 215
学习任务1　路由器广域网协议的封装配置 …… 216
学习活动1　路由器广域网HDLC封装配置 …… 216
学习活动2　路由器广域网PPP封装配置 …… 220
学习任务2　路由器广域网协议的PPP封装验证 …… 226
学习活动1　使用PPP的PAP认证 …… 226
学习活动2　使用PPP的CHAP认证 …… 231
学习任务3　网络地址转换协议配置 …… 236
学习活动1　利用NAT实现外网主机访问内网服务器 …… 236
学习活动2　利用动态NAT实现局域网访问互联网 …… 240
项目6　无线网络配置 …… 247
学习任务1　配置瘦AP模式的无线网络 …… 247
学习任务2　无线AC的DHCP服务管理 …… 255
学习任务3　无线AC的安全控制 …… 257
项目7　防火墙的配置 …… 262
学习任务1　防火墙基本配置 …… 262
学习活动1　防火墙初级管理 …… 263
学习活动2　防火墙典型环境安全策略实施 …… 267
学习任务2　实现防火墙上的VPN技术 …… 270
学习活动1　实现防火墙的SSL VPN技术 …… 270
学习活动2　实现防火墙IPSec VPN技术 …… 278
项目8　综合实战 …… 286
学习任务1　小型企业的网络工程案例 …… 286
学习任务2　企业网络综合实战 …… 292



IP 地址规划

项目学习说明

随着信息化的高速发展，人们把越来越多的事务转移到网络平台上。小到一个家庭，大到一个学校、企业，为了提高工作效率，共享信息资源，需要构建一个局域网络，合理地规划和使用 IP 地址。要构建简单的局域网络，需要掌握配置 IP 地址参数等基本知识与技能。

本项目重点学习部门间 IP 地址规划和合理利用 IP 地址的方法。

学习能力目标

学习任务 1　部门间 IP 地址规划
学习任务 2　合理利用 IP 地址

职业能力目标

- 能理解 IP 地址的分类
- 能规划和合理使用 IP 地址

学习任务 1　部门间 IP 地址规划

学习情境

某公司内设有技术部、学术部、销售部三个部门，每个部门均有 20 台计算机，且 ISP 已分配地址段 192.168.10.0/24 给该公司使用，请充分考虑网络的性能及管理效率等因素，对该网络的 IP 地址进行规划。

情境分析

从任务描述中可得知，公司的三个部门拥有计算机数量均为 20 台，且从 ISP 处获得一个 C 类 IP 地址段。从网络性能方面考虑，应尽量缩减网络流量，把部门内部通信业务尽量“圈定”在部门内部进行；从日常管理的角度考虑，把一个较大的网络分成相对较小的网络有利于隔离和排除故障。因此，可以考虑通过合理的子网划分来解决问题。

本任务需要完成的几个主要步骤如下。

（1）确定各子网的主机数量。

① 每台 TCP/IP 主机至少需要一个 IP 地址。

② 路由器每个接口各需要一个 IP 地址。

（2）确定每个子网的大小。

（3）基于以上需要，创建以下内容。

① 为整个网络设定一个子网掩码。

② 为每个物理网段设定一个子网 ID。

③ 为每个子网确定主机的合法地址范围。

公司网络拓扑结构如图 1-1-1 所示。

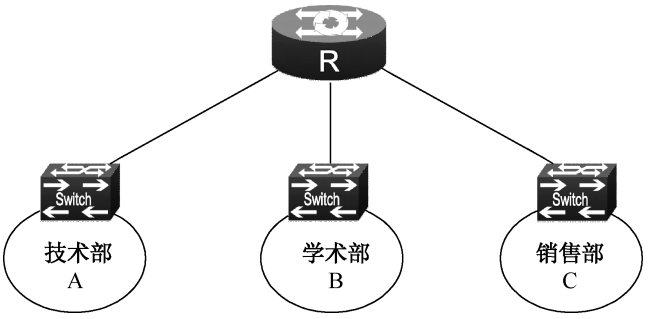


图 1-1-1　公司网络拓扑结构

相关知识

1. 子网掩码的分类

子网掩码共两类：一类是默认子网掩码，另一类是自定义子网掩码。默认子网掩码即未划分子网，对应的网络号的位都设置为 1，主机号都设置为 0。

A 类网络默认子网掩码：255.0.0.0。

B 类网络默认子网掩码：255.255.0.0。

C 类网络默认子网掩码：255.255.255.0。

自定义子网掩码是将一个网络划分为几个子网，需要每一段使用不同的网络号或子网号，实际上可以认为将主机号分为两个部分：子网号、子网主机号。其形式如下。

未做子网划分的 IP 地址：网络号 + 主机号

做子网划分后的 IP 地址：网络号 + 子网号 + 子网主机号

也就是说，IP 地址在划分子网后，以前的主机号位置的一部分给了子网号，余下的是子

网主机号。子网掩码是 32 位二进制数，它的子网主机标识部分为全“ 0 ”。利用子网掩码可以判断两台主机是否在同一子网中。若两台主机的 IP 地址分别与它们的子网掩码相“ 与 ”后的结果相同，则说明这两台主机在同一子网中。

2. 子网掩码的表示方法

子网掩码通常有以下两种格式的表示方法：通过与 IP 地址格式相同的点分十进制表示，如 255.0.0.0 或 255.255.255.128；在 IP 地址后加上“ / ”符号以及 1～22 的数字，其中 1～32 的数字表示子网掩码中网络标识位的长度，如 192.168.10.1/24 的子网掩码也可以表示为 255.255.255.0。

3. 子网划分的捷径

（1）确定所选择的子网掩码将会产生多少个子网。

N=2x－2（x 代表掩码位，即二进制为 1 的部分），现在的网络中已经不需要－2，可以全部使用，不过需要加上相应的配置命令，如 Cisco 路由器加上 ip subnet zero 命令就可以全部使用。

（2）每个子网能有多少台主机。

M=2 y –2（y 代表主机位，即二进制为 0 的部分）。

（3）有效子网 ID 计算。

① 计算出地址的分段基数（分段大小）：分段基数=256－十进制的子网掩码。

② 有效子网 ID=n×分段基数，（n=1，2，…），如子网掩码为 255.255.255.224，则分段基数为 256－224=32, 第一个有效子网 ID 为 192.168.10.32, 第二个有效子网 ID 为 192.168.10（2×32=64），以此类推。

（4）每个子网的广播地址：广播地址=下个子网号－1。

（5）每个子网的有效主机。

忽略子网内全为 0 和全为 1 的地址剩下的就是有效主机地址，有效主机地址=下个子网号－2（即广播地址－1）。

早期的互联网使用的路由产品不支持全 0 或者全 1 的 IP，但是新的产品都支持，这样就涉及兼容的问题。如果在使用的网络当中能够确定没有陈旧的路由产品（包括路由器、交换机、操作系统）存在，可抛开 RFC 950 和 RFC 1122 标准，遵守 RFC 1812 的标准使用全 0 或者全 1 的 IP 地址。

步骤实现

（1）确定各子网的主机数量。IPv4 中地址是由 32 位二进制位组成的，且分为网络位和主机位两部分，如图 1-1-2 所示。

图 1-1-2　IP 地址结构

由前文分析可知，每个部门各需要 21 个 IP 地址，其中 20 个为计算机使用，1 个为路由器端口使用。

（2）确定每个子网的大小。十进制 21 至少需要 5 位二进制数来表达，于是我们可以确定

子网的大小为 2^5=32。子网大小示意图如图 1-1-3 所示。

（3）创建子网掩码、子网 ID、合法 IP 范围。

① 为整个网络设定子网掩码。将图 1-1-3 中网络位的二进制值全部设置为 1，主机位的二进制值全部设置为 0，即可得到划分子网后的子网掩码。计算过程如图 1-1-4 所示。

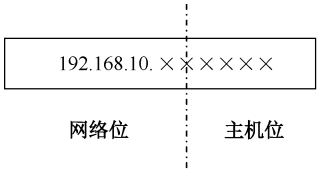


图 1-1-3　子网大小示意图

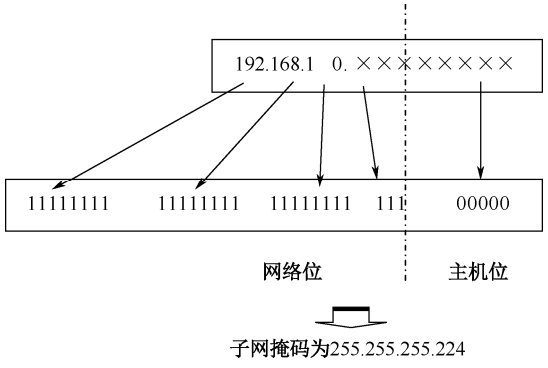


图 1-1-4　子网掩码计算过程

② 为每个物理网段设定一个子网 ID。RFC 标准规定，子网的网络 ID 不能为全“ 0 ”或全“ 1 ”，合法的子网 ID 如图 1-1-5 所示。

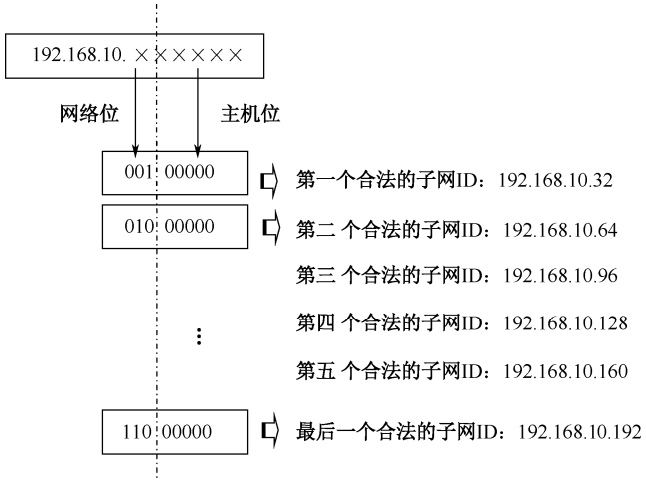


图 1-1-5　子网 ID 计算过程

③ 为每个子网确定主机的合法地址范围。RFC 规定，主机 ID 不能为全“ 0 ”或全“ 1 ”，下面以第一个合法子网为例说明子网中主机 ID 的计算过程。具体过程如图 1-1-6 所示。

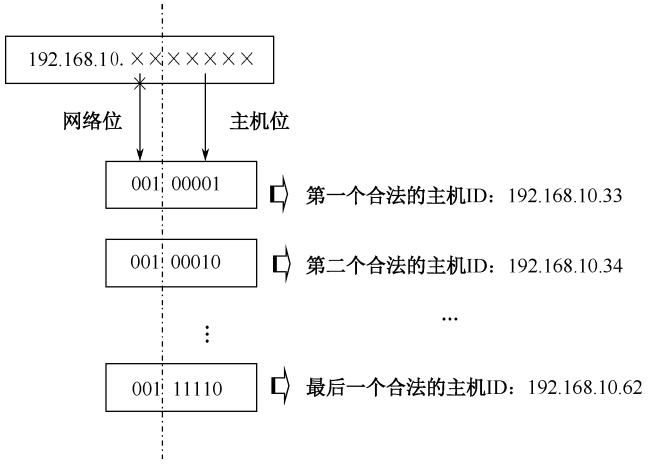


图 1-1-6　第一个合法子网中的合法主机 ID 计算过程

经计算得出本任务三个部门拟使用的子网中合法 ID 见表 1-1-1～表 1-1-3。

表 1-1-1　子网 192.168.10.32

子　网	主　机	意　义
192.168.10.32/24	192.168.10.32	子网的网络地址
	192.168.10.33	子网中第一个合法的主机 ID
	192.168.10.62	子网中最后一个合法的主机 ID
	192.168.10.63	子网的广播地址

表 1-1-2　子网 192.168.10.64

子　网	主　机	意　义
192.168.10.64	192.168.10.64	子网的网络地址
	192.168.10.65	子网中第一个合法的主机 ID
	192.168.10.94	子网中最后一个合法的主机 ID
	192.168.10.95	子网的广播地址

表 1-1-3　子网 192.168.10.96

子　网	主　机	意　义
192.168.10.96	192.168.10.96	子网的网络地址
	192.168.10.97	子网中第一个合法的主机 ID
	192.168.10.126	子网中最后一个合法的主机 ID
	192.168.10.127	子网的广播地址

（4）经以上计算该公司三个部门的 IP 地址，规划如图 1-1-7 所示。

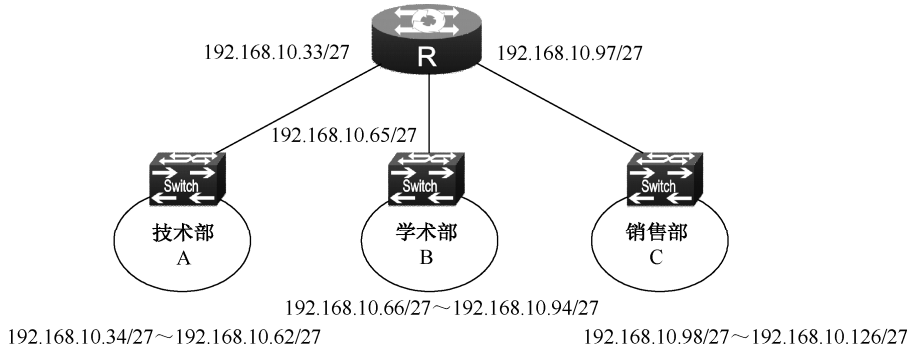


图 1-1-7　公司网络各部门 IP 地址整体规划

课堂训练

一家集团公司有 12 家子公司，每家子公司又有四个部门。上级给出一个 172.16.0.0/16 的网段，以给每家子公司以及子公司的部门分配网段。

思路：既然有 12 家子公司，那么要划分 12 个子网段，但是每家子公司又有四个部门，因此又要在每家子公司所属的网段中划分四个子网分配给各部门。

（1）可划分出 16 个子网。

① **10101100.00010000.0000**0000.00000000/20【172.16.0.0/20】。

② **10101100.00010000.0001**0000.00000000/20【172.16.16.0/20】。

③ **10101100.00010000.0010**0000.00000000/20【172.16.32.0/20】。

④ **10101100.00010000.0011**0000.00000000/20【172.16.48.0/20】。

⑤ **10101100.00010000.0100**0000.00000000/20【172.16.64.0/20】。

⑥ **10101100.00010000.0101**0000.00000000/20【172.16.80.0/20】。

⑦ **10101100.00010000.0110**0000.00000000/20【172.16.96.0/20】。

⑧ **10101100.00010000.0111**0000.00000000/20【172.16.112.0/20】。

⑨ **10101100.00010000.1000**0000.00000000/20【172.16.128.0/20】。

⑩ **10101100.00010000.1001**0000.00000000/20【172.16.144.0/20】。

⑪ **10101100.00010000.1010**0000.00000000/20【172.16.160.0/20】。

⑫ **10101100.00010000.1011**0000.00000000/20【172.16.176.0/20】。

⑬ **10101100.00010000.1100**0000.00000000/20【172.16.192.0/20】。

⑭ **10101100.00010000.1101**0000.00000000/20【172.16.208.0/20】。

⑮ **10101100.00010000.1110**0000.00000000/20【172.16.224.0/20】。

⑯ **10101100.00010000.1111**0000.00000000/20【172.16.240.0/20】。

（2）以下仅以甲公司为例，其他子公司情况略。错两位后（可划分出四个子网）：

① 10101100.00010000.00000000.00000000/22【172.16.0.0/22】。

② 10101100.00010000.00000100.00000000/22【172.16.4.0/22】。

③ 10101100.00010000.00001000.00000000/22【172.16.8.0/22】。

④ 10101100.00010000.00001100.00000000/22【172.16.12.0/22】。

学习小结

本学习任务介绍了部门间 IP 地址的规划，通过对 IP 地址的规划，把较大的网络进行隔离，有利于排除故障，同时也节省了 IP 地址的数量，IP 地址的规划在企业中使用较多，需要熟练掌握。

学习任务 2　合理使用 IP 地址

学习情境

某跨国公司下设“珠海总公司”“广州分公司”和“西雅图分公司”。珠海总公司拥有计算机 80 台，广州分公司拥有计算机 23 台，西雅图分公司拥有计算机 50 台，且 ISP 已分配地址段 192.168.1.0/24 给该公司使用，请充分考虑网络的性能以及管理效率等因素，对该网络的 IP 地址进行规划。

情境分析

从任务描述中可得知，该公司的三个办公地点的计算机数量差异较大，珠海总公司所需的主机数量最多，至少应该划分一个大小为 96 的地址块供其使用，如果依据划分子网的方法（即定长子网），则所需的 IP 地址为 96×3=288，但 ISP 只提供了一个 C 类 IP 地址段，IP 地址数量为 255。由 255<288 可知，定长子网划分在本任务中无法胜任，本任务可以考虑通过变长子网划分来解决问题。

本任务需要完成的几个主要步骤如下。

（1）确定各子网的主机数量。

① 每台 TCP/IP 主机至少需要一个 IP 地址。

② 路由器每个接口各需要一个 IP 地址。

（2）确定每个子网的大小。

（3）基于以上需要，创建以下内容。

① 为每个子网设定一个子网掩码。

② 为每个物理网段设定一个子网 ID。

③ 为每个子网确定主机的合法地址范围。

网络拓扑结构如图 1-2-1 所示。

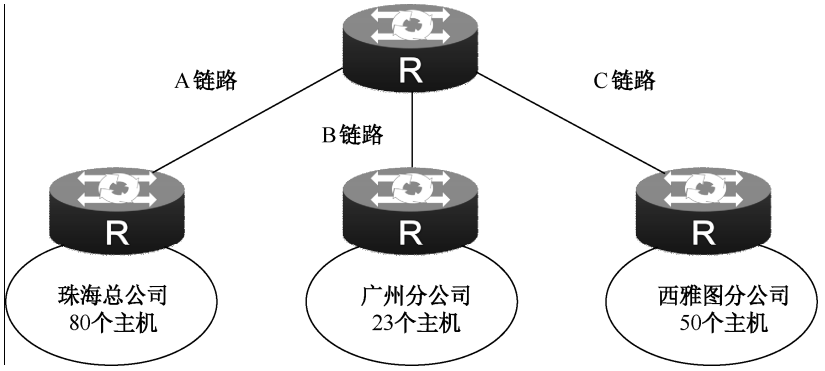


图 1-2-1　公司网络拓扑

相关知识

什么是 VLSM

VLSM 即可变长子网掩码，是为了解决在一个网络系统中使用多种层次子网化 IP 地址的问题而发展起来的。这种策略只能在所用的路由协议都支持的情况才能使用，如开放式最短路径优先路由选择（OSPF）协议和增强内部网关路由选择协议（EIGRP）。RIP 版本 1 由于出现早于 VLSM 而无法支持，RIP 版本 2 可以支持 VLSM。

VLSM 允许一个组织在同一个网络地址空间中使用多个子网掩码。利用 VLSM 可以实现“把子网继续划分为子网”功能，使寻址效率达到最高。

步骤实现

（1）确定各子网的主机数量，见表 1-2-1。

表 1-2-1　主机数量

子　　网	主机数量	作　　用
珠海总公司	81	其中一个 IP 地址分配给路由器的接口
广州分公司	24	
西雅图分公司	51	
A 链路	2	
B 链路	2	
C 链路	2	

（2）确定每个子网的大小，见表 1-2-2。

表 1-2-2　子网大小

子　　网	主机数量	子网大小	备　　注
珠海总公司	81	128	
广州分公司	24	32	
西雅图分公司	51	64	

续表

子　　网	主机数量	子网大小	备　　注
A 链路	2	4	子网中至少需要四个主机 ID，否则除了网络 ID 和广播地址外无 IP 地址可用
B 链路	2	4	
C 链路	2	4	

（3）创建子网掩码、子网 ID、合法 IP 地址范围。

划分子网的思路如下：首先为较大子网分配地址块，然后从未被分配的地址块中为剩下的较大子网分配地址块，以此类推（注意，此处将使用 1 子网和 0 子网），思路如图 1-2-2 所示。

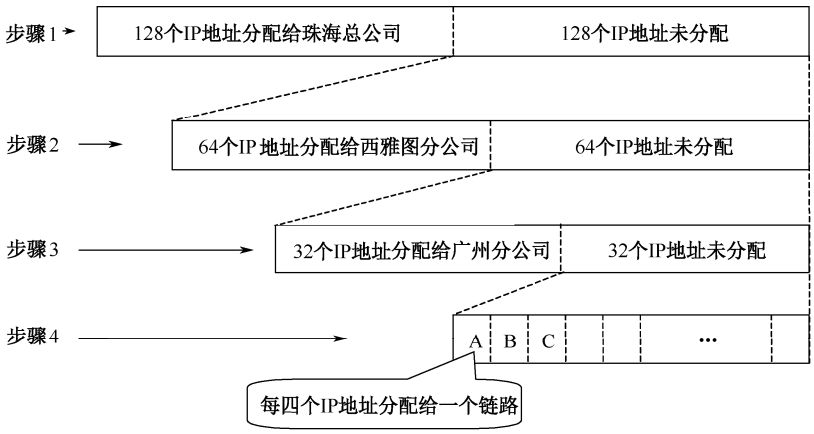


图 1-2-2　变长子网划分思路

① 为每个子网设定子网掩码。

a．珠海总公司所需地址块为 128，即需要 7 位二进制位，故子网位为 1 位二进制位，子网掩码计算过程如图 1-2-3 所示。

b．西雅图分公司所需地址块为 64，即需要 6 位二进制位，故子网位为 2 位二进制位，子网掩码计算过程如图 1-2-4 所示。

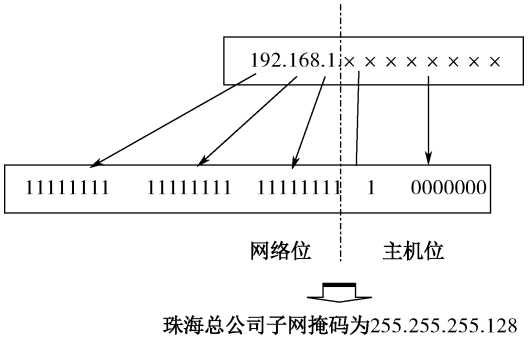


图 1-2-3　珠海总公司子网掩码计算过程

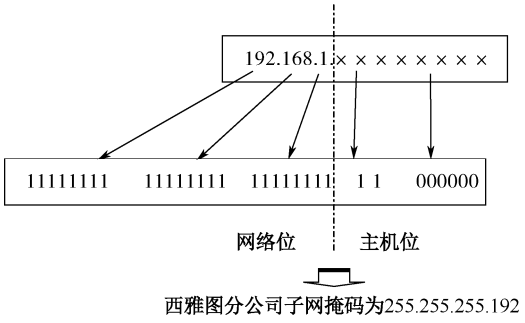


图 1-2-4　西雅图分公司子网掩码计算过程

c．广州分公司子所需地址块为 32，即需要 5 位二进制位，故子网位为 3 位二进制位。子网掩码计算过程如图 1-2-5 所示。

d. A、B、C 链路所需地址块为 4，即需要 2 位二进制位，故子网位为 6 位二进制位，子网掩码计算过程如图 1-2-6 所示。

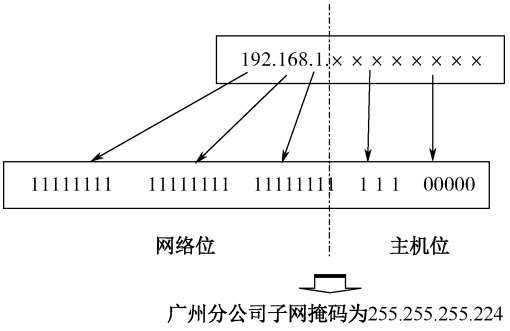


图 1-2-5　广州分公司子网掩码计算过程

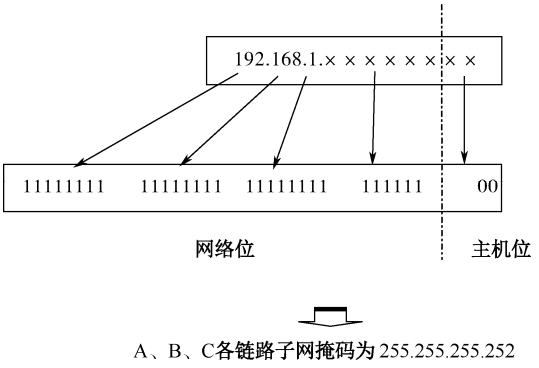


图 1-2-6　A、B、C 各链路子网掩码计算过程

② 为每个物理网段设定一个子网 ID，如图 1-2-7 所示。

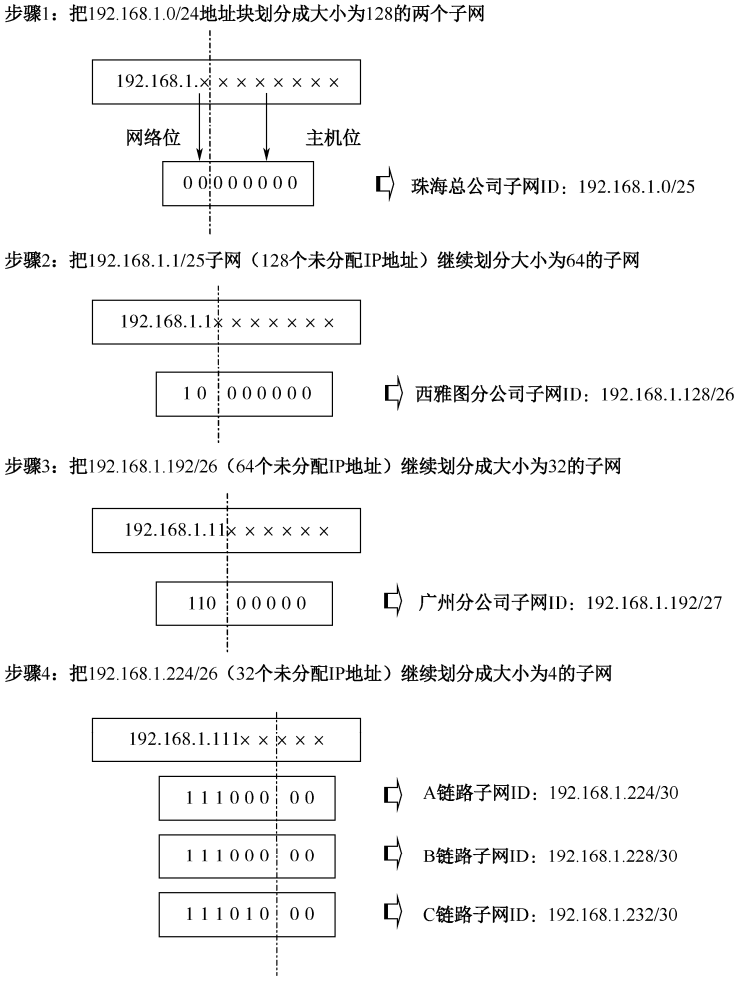


图 1-2-7　子网 ID 计算过程

③ 为每个子网确定主机的合法地址范围。

经计算得出本任务 7 个子网的合法 ID，见表 1-2-3～表 1-2-6。

表 1-2-3　子网 192.168.1.0/25

子　网	部　门	主　机	意　义
192.168.1.0/25	珠海总公司	192.168.1.0/25	子网的网络地址
		192.168.1.1/25	子网中第一个合法的主机 ID
		192.168.1.126/25	子网中最后一个合法的主机 ID
		192.168.1.127/25	子网的广播地址

表 1-2-4　子网 192.168.1.128/26

子　网	部　门	主　机	意　义
192.168.1.128/26	西雅图分公司	192.168.1.128/26	子网的网络地址
		192.168.1.129/26	子网中第一个合法的主机 ID
		192.168.1.190/26	子网中最后一个合法的主机 ID
		192.168.1.191/26	子网的广播地址

表 1-2-5　子网 192.168.1.192/27

子　网	部　门	主　机	意　义
192.168.1.192/27	广州分公司	192.168.1.192/27	子网的网络地址
		192.168.1.193/27	子网中第一个合法的主机 ID
		192.168.1.222/27	子网中最后一个合法的主机 ID
		192.168.1.223/27	子网的广播地址

表 1-2-6　链路子网 A～C

子　网	部　门	主　机	意　义
192.168.1.224/30	链路子网 A	192.168.1.224/30	子网的网络地址
		192.168.1.225/30	子网中第一个合法的主机 ID
		192.168.1.226/30	子网中最后一个合法的主机 ID
		192.168.1.227/30	子网的广播地址
192.168.1.228/30	链路子网 B	192.168.1.228/30	子网的网络地址
		192.168.1.229/30	子网中第一个合法的主机 ID
		192.168.1.230/30	子网中最后一个合法的主机 ID
		192.168.1.231/30	子网的广播地址
192.168.1.232/30	链路子网 C	192.168.1.232/30	子网的网络地址
		192.168.1.233/30	子网中第一个合法的主机 ID
		192.168.1.234/30	子网中最后一个合法的主机 ID
		192.168.1.235/30	子网的广播地址

（4）经以上计算该公司三个部门的 IP 地址规划如图 1-2-8 所示。

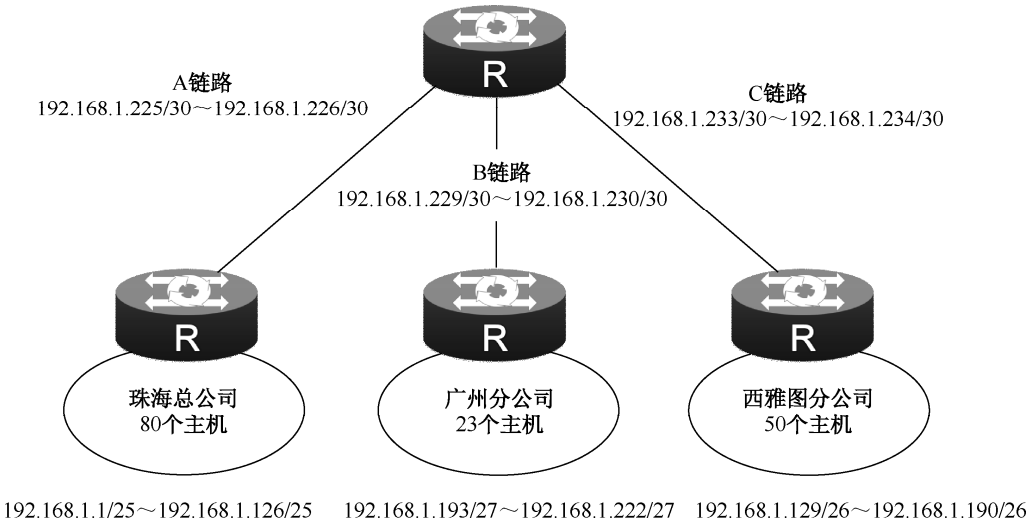


图 1-2-8　公司网络 IP 地址规划图

课堂训练

某集团公司给下属子公司甲分配了一段 IP 地址 192.168.5.0/24，现在甲公司有两层办公楼（1 楼和 2 楼），统一从 1 楼的路由器接入公网。1 楼有 100 台计算机联网，2 楼有 53 台计算机联网。如果你是该公司的网管，应该怎么去规划这个 IP 地址段？

思路：

（1）在划分子网时优先考虑使用最大主机数来划分（101 个可用 IP 地址，则要保证至少 7 位的主机位可用 $2^m-2\geq 101$，m 的最小值为 7）。如果保留 7 位主机位，则只能划分出两个网段，剩下的一个网段就划分不出来了。但是我们剩下的一个网段只需要 2 个 IP 地址并且 2 楼的网段只需要 54 个可用 IP，因此，我们可以从第一次划分的两个网段中选择一个网段来继续划分 2 楼的网段和路由器互连使用的网段。

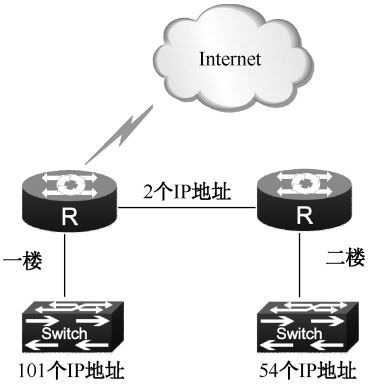


图 1-2-9　网络拓扑结构图

（2）网络拓扑结构如图 1-2-9 所示。

完成标准见表 1-2-7。

表 1-2-7　某集团公司 IP 地址划分

子　网	网络地址	有效 IP 地址	广播地址
1 楼	192.168.5.0/25	192.168.5.1/25～192.168.5.126/25	192.168.5.127/25
2 楼	192.168.5.128/26	192.168.5.129/26～192.168.5.190/26	192.168.5.191/26
链路	192.168.5.192/30	192.168.5.193/30～192.168.5.194/30	192.168.5.195/30

学习小结

本学习任务介绍了怎样合理使用 IP 地址，通过 VLSM 对子网进行划分，使寻址效率达到最高，提高了网络性能和管理效率，在企业中应用较多，需要熟练掌握。

项目考核

某公司拟新建公司办公网络，从 ISP 处获得一段 C 类地址块 192.168.10.0/24，试根据图 1-2-10 中描述的信息对该公司网络进行适当的网络地址规划。制作网线连接子网 A 中的 PC1 和 PC2，安装适当的协议，配置相应的 IP 地址信息，进行必要的测试，使 PC1 能访问 PC2 中的共享文件夹。

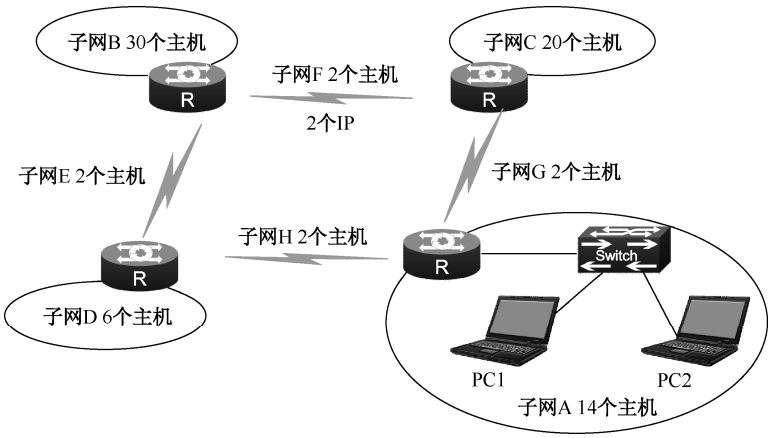
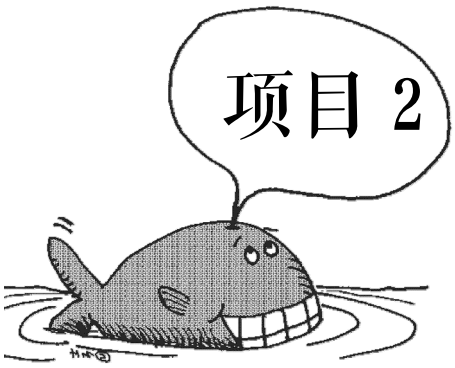


图 1-2-10　网络拓扑图

根据拓扑结构图完成各子网的 IP 地址计算与子网划分。完成所需网线的制作，并按拓扑连接网络设备。公司 IP 地址规划见表 1-2-8。

表 1-2-8　某公司 IP 地址规划

子　网	网络地址	有效 IP 地址	广播地址
A 子网	192.168.10.16/28		
B 子网	192.168.10.32/27		
C 子网	192.168.10.64/27		
D 子网	192.168.10.8/29		
E 子网	192.168.10.96/30		
F 子网	192.168.10.100/30		
G 子网	192.168.10.104/30		
H 子网	192.168.10.108/30		



交换机的配置

项目学习说明

交换机是网络的核心设备之一，它是一种基于物理地址识别，并能完成封装转发数据包功能的网络设备。交换机可以让不同地理位置的不同部门之间进行协同办公，以智能化和信息化的办公网络系统实现资源共享，极大地提高了部门间的工作效率，使办公变得更加便捷和轻松。

本项目重点学习交换机的基本配置、交换机的 VLAN 配置、交换机的常用技术和交换机间的路由配置。

学习能力目标

学习任务 1 交换机的基本配置
学习任务 2 交换机的 VLAN 配置
学习任务 3 交换机的常用技术
学习任务 4 交换机的路由配置

职业能力目标

- 熟练掌握交换机的基本配置命令
- 熟练掌握交换机的 VLAN 配置命令
- 理解二层和三层交换机的区别和联系
- 熟练掌握链路聚合，以增加交换机之间的带宽
- 熟练掌握交换机的路由配置命令

学习任务 1　交换机的基本配置

交换机的基本配置主要有设备命名、登录信息、设置特权密码、VTY 密码、Telnet 管理和端口配置等。本学习任务分成以下三个学习活动进行。

学习活动 1　交换机的管理方式。

学习活动 2　交换机的简单配置。

学习活动 3　交换机文件的备份和保存。

学习活动 1　交换机的管理方式

交换机的管理方式可以分为带内管理与带外管理。通过交换机的 Console 口管理交换机属于带外管理，特点是无须占用交换机的网络接口，但线缆特殊，配置距离短。带内管理主要分为 Telnet、Web 与 SNMP。

学习情境

现因公司业务发展需求，需要购买一台交换机扩展现有网络，根据公司的网络拓扑规划，网络管理员将刚买回来的新交换机经过配置后，即可投入使用。

情境分析

管理员拿到刚买的交换机，第一次对出厂的交换机进行配置时，可以通过交换机的 Console 口进行配置。在交换机上有一个 Console 口，可从交换机端口标识中识别，之后可通过出厂自带的配置线进行连接和配置。

所需设备如下。

（1）DCS-3950 交换机 1 台。

（2）PC1 台。

（3）Console 线 1 条。

学习活动的拓扑结构如图 2-1-1 所示。

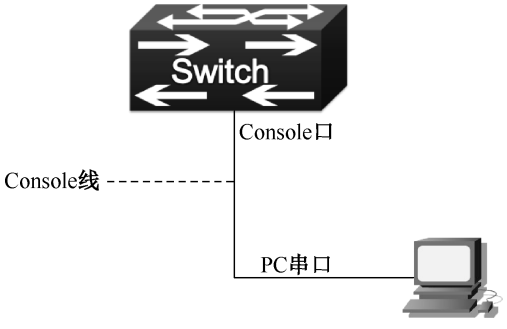


图 2-1-1　交换机带外配置

相关知识

（1）默认情况下交换机的所有端口属于 VLAN1。

（2）交换机的传输模式有全双工、半双工、全双工/半双工自适应。交换机的全双工是指交换机在发送数据的同时也能够接收数据，两者同步进行，这好像打电话，说话的同时也能够听到对方的声音。一般而言，交换机支持全双工。全双工的好处在于迟延小、速度快。

（3）可网管交换机上都有一个 Console 口，它是专门用于对交换机进行配置和管理的端口。配置 PC 通过 Console 口和交换机连接，以配置和管理可网管交换机。Console 口的类型绝大多数采用 RJ-45 端口，需要通过专门的 Console 线连接到配置 PC 的串口上，使配置 PC 成为超级终端。

（4）show 命令。

show vers：查看交换机的版本信息。

show running-config：查看交换机的配置信息。

（5）交换机出厂第一次启动，进入“ setup configuration ”，用户可以选择进入 setup 模式或者跳过 setup 模式。键入“ y ”，按【Enter】键就会进入 setup 模式。

用户在进入主菜单之前，会提示用户选择配置界面的语言种类，对英文不是很熟悉的用户可以选择“ 1 ”，进入中文提示的配置界面。选择“ 0 ”则进入英文提示的配置界面。

```
Please select language
[0]:English
[1]:中文
Selection(0|1) [0]:
```

具有中文提示的配置界面是神州数码网络产品本土化的重要特色。

（6）为了对网络进行有效的保护，允许用户以不同的身份登录交换机进行配置，允许对不同的身份设置不同的密码，不同的身份在配置交换机时有不同的权限。目前，神州数码的交换机可以设置 visitor 和 admin 两种身份。

visitor 登录身份的配置权限：支持 show、ping、traceroute、clear 等命令，该身份无法进入 config 模式。admin 登录身份的配置权限支持所有的命令。

进入特权模式命令：enable [level {visitor|admin} [<password>]]，用来指定身份及密码登录交换机。设置登录身份的相关密码：enable password level {visitor|admin}，指定登录配置模式的密码。

（7）交换机的配置模式。

① 用户模式 :用户进入 CLI 界面, 首先进入的是一般用户配置模式, 提示符为“ switch> ”，符号“ > ”为一般用户配置模式的提示符。当用户从特权用户配置模式使用命令 exit 退出时，可以回到一般用户配置模式。用户在一般用户配置模式下不能对交换机进行任何配置，只能查询交换机基本信息。

② 特权模式：在一般用户配置模式下使用 enable 命令，如果已经配置了进入特权用户的口令，则输入相应的特权用户口令，即可进入特权用户配置模式“ switch# ”。当用户从全局配置模式使用 exit 退出时，也可以回到特权用户配置模式。

在特权用户配置模式下，用户可以查询交换机配置信息、各个端口的连接情况、收发数据统计等。进入特权用户配置模式后，可以用全局配置模式对交换机的各项配置进行修改，

因此进行特权用户配置模式必须要设置特权用户口令，防止非特权用户的非法使用，对交换机配置进行恶意修改，造成不必要的损失。

③ 全局模式：进入特权用户配置模式后，只需使用命令 config，即可进入全局配置模式“ switch(config)# ”。当用户在其他配置模式，如接口配置模式、VLAN 配置模式时，可以使用命令 exit 退回全局配置模式。

（8）交换机 CLI 其他使用方式。

① CLI 快捷键。【Backspace】用于删除光标所在位置的前一个字符，上光标键【↑】显示上一个输入命令，最多可显示最近输入的十个命令，下光标键【↓】显示下一个输入命令。当使用上光标键回溯到以前输入的命令时，也可以使用下光标键后退。左光标键【←】为光标向左移动一个位置。右光标键【→】为光标向右移动一个位置。左右键的配合使用，可对已输入的命令做覆盖修改。

【Ctrl+Z】组合键从其他配置模式（一般用户配置模式除外）直接退回到特权用户模式。

【Ctrl+C】组合键打断交换机 ping 或其他正在执行的命令进程。

当输入的字符串可以无冲突地表示命令或关键字时，可以使用【Tab】键将其补充成完整的命令或关键字。

//执行上上一级目录的命令。

② CLI 帮助功能。在任一命令模式下，输入“ ？ ”，获取该命令模式下的所有命令及其简单描述。在命令的关键字后，输入以空格分隔的“ ？ ”，若该位置是参数，则会输出该参数的类型、范围等描述；若该位置是关键字，则列出关键字的集合及其简单描述；若输出“ <cr> ”，则此命令已输入完整，在该处按【Enter】键即可。在字符串后紧接着输入“ ？ ”，会列出以该字符串开头的所有命令。

③CLI 对输入的检查。通过键盘输入的所有命令都要经过 Shell 检查，正确地输入命令，且执行成功，不会显示任何信息。

④常见错误返回信息。

```
Unrecognized command or illegal parameter!
```

命令不存在，或者参数的范围、类型、格式有错误。

```
Ambiguous command
```

根据已有输入可以产生至少两种不同的解释。

```
Invalid command or parameter
```

命令解析成功，但没有任何有效的参数记录。

```
This command is not exist in current  mode
```

命令可解析，但当前模式下不能配置该命令

⑤CLI 支持不完全匹配。绝大部分交换机的 Shell 支持不完全匹配的搜索命令和关键字，当输入无冲突的命令或关键字时，Shell 就会正确解析。

例如，对特权用户配置命令“ show interface ethernet 1 ”只要输入“ sh in e 1 ”即可。

步骤实现

1. 交换机的带外管理方式

步骤 1：连接 Console 线。

拔插 Console 口线时注意保护交换机的 Console 口和 PC 的串口，不要带电拔插。

步骤 2：使用超级终端进入交换机。

（1）执行“开始”→“程序”→“附件”→“通信”→“超级终端”命令。

（2）为建立的超级终端连接命名：输入新建连接的名称，系统会为用户把这个连接保存在附件的通信栏中，以便于用户的下次使用，单击“确定”按钮，如图 2-1-2 所示。

（3）选择所使用的端口号：在“名称”文本框中输入“DCS-3950”，“连接时使用”默认设置连接在“COM1”口上，单击其下拉按钮，可根据用户实际连接的端口而定，如图 2-1-3 所示。

图 2-1-2　超级终端

图 2-1-3　连接串行接口

（4）设置端口属性。单击右下方的“还原为默认值”按钮，每秒位数为“9600”，数据位为“8”，奇偶校验为“无”，停止位为“1”，数据流控制为“无”，如图 2-1-4 所示。

（5）如果 PC 串口与交换机的 Console 口连接正确，只要在超级终端按【Enter】键，将会弹出如图 2-1-5 所示的窗口，表示已经进入了交换机，此时已经可以对交换机输入指令进行查看。

图 2-1-4　设置串行接口属性

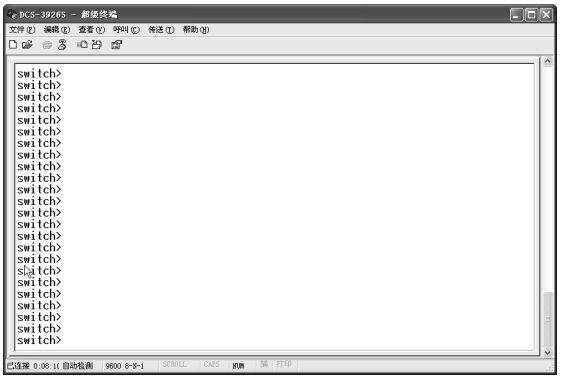


图 2-1-5　交换机命令行 CLI 界面

（6）此时，用户已经成功进入交换机的配置界面，可以对交换机进行必要的配置。使用“show ver”命令可以查看交换机的软硬件版本信息，如图 2-1-6 所示。

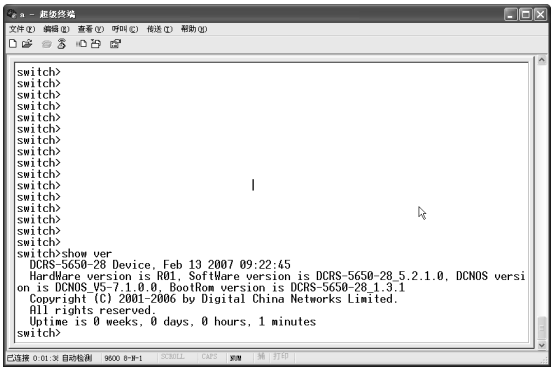

超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)
switch>
switch>show ver
DCRS-5650-28 Device, Feb 13 2007 09:22:45
HardWare version is R01, SoftWare version is DCRS-5650-28_5.2.1.0, DCNOS version is DCNOS_V5-7.1.0.0, BootRom version is DCRS-5650-28_1.3.1
Copyright (C) 2001-2006 by Digital China Networks Limited.
All rights reserved.
Uptime is 0 weeks, 0 days, 0 hours, 1 minutes
switch>
已连接 0:01:36 自动检测 9600 8-N-1

图 2-1-6　使用“ show ver ”命令显示版本信息

（7）使用“ show running-config ”命令查看当前配置。

```
switch>enable                    ！进入特权配置模式
switch#show running-config       ！显示交换机的配置信息
current configuration
!
hostname switch
!
!
vlan 1
        vlan1
!
!
interface ethernet0/0/1
!
interface ethernet0/0/2
!
interface ethernet0/0/3
!
.
.
.
```

知识拓展

使用 Telnet 方式管理交换机的所需设备如下：

（1）DCS-3950 交换机 1 台。

（2）PC 1 台。

（3）Console 线 1 条。

（4）直通双绞线 1 条。

实验拓扑结构如图 2-1-7 所示。

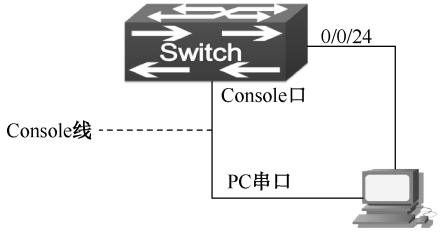


图 2-1-7　Telnet 方式管理交换机

步骤 1：设置 PC 网卡的 IP 地址为 192.168.1.101/24，子网掩码为 255.255.255.0。

步骤 2：交换机恢复出厂设置。

```
switch#set default                          ！恢复出厂设置
Are you sure ? [Y/N]=y
switch#write                                ！保存配置
switch#reload                               ！重启交换机
Process with reboot ?[Y/N]y                 ！输入“y”
```

步骤 3：设置正确的时钟和名称。

```
switch#clock set 15:29:50 2010.01.16        ！设置交换机系统时钟
switch#                                     ！交换机特权模式
switch#config                               ！进入交换机全局模式
switch(config)#hostname DCS-3950            ！将交换机命名为DCS-3950
DCS-3950(config)#exit
```

步骤 4：设置交换机的管理地址。

```
DCS-3950#config
DCS-3950(config)#interface vlan 1           ！进入VLAN1的接口
DCS-3950(Config-if-Vlan1)#ip address 192.168.1.100  255.255.255.0
                                            ！配置VLAN1的IP地址
DCS-3950(Config-if-Vlan1)#no shutdown       ！开启该接口
DCS-3950(Config-if-Vlan1)#exit
```

小贴士

命令“no shutdown”用于开启交换机某端口，配置好接口后，还需要启用端口才能生效，与之对应的关闭端口的命令为“shutdown”。

步骤 5：为交换机设置授权 Telnet 用户。

```
DCS-3950#config
DCS-3950(config)#telnet-user xuxp password 0 digital
                                ！设置Telnet用户名和密码，并且密码不加密
DCS-3950(config)#exit
DCS-3950#
```

小贴士

（1）命令“telnet-user xuxp password 0 digital”中，数字“0”表示密码不加密显示，如

果更改为数字“7”，则表示密码加密。“xuxp”为用户名，“digital”为密码，密码只能是 1～8 个字符。

（2）删除一个 Telnet 用户可以在 config 模式下使用 no telnet-user 命令。

（3）命令“telnet-server enable”用于打开交换机的 Telnet 服务器功能，该命令只能在 Console 下使用，管理员使用本命令允许或者拒绝 Telnet 客户端登录到交换机。本命令的“no”操作具有关闭交换机的 Telnet 服务器功能。系统默认打开 Telnet 服务器功能。注意，本命令是在 DCRS-5650-28 系列下操作实现的，至于其他系列请读者自行尝试。

（4）命令“telnet-server security ip”，配置交换机作为 Telnet 服务器允许登录的 Telnet 客户端的安全 IP 地址，本命令的“no”操作为删除指定的 Telnet 客户端的安全 IP 地址。注意，本命令是在 DCRS-5650-28 系列下操作实现的，至于其他系列请读者自行尝试。

步骤 6：验证主机与交换机是否连通。

```
DCS-3950#ping 192.168.1.101
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 192.168.1.101, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1ms
```

！5个感叹号表示5个包都ping通了，如图2-1-8所示。

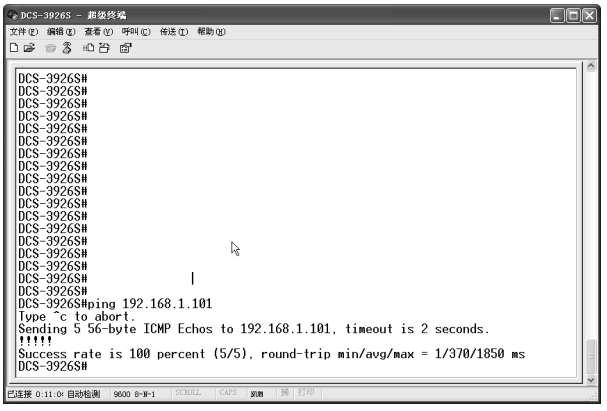


图 2-1-8　ping 测试

步骤 7：Telnet 测试。

（1）执行“开始”→“运行”命令，在“打开”文本框中输入“telnet 192.168.1.100”，如图 2-1-9 所示。

图 2-1-9　运行 Telnet 命令

（2）在“Username”文本框中输入“xuxp”，在“Password”文本框中输入“digital”，如图 2-1-10 所示，显示“switch>”表示远程登录成功。

图 2-1-10　Telnet 方式管理交换机

学习小结

本学习活动介绍了交换机的管理方式，需要注意的是，管理方式有 Console 口、Telnet、HTTP 等方式，但初始化的交换机一般使用 Console 方式，对交换机进行了相关的配置后，就可以使用 Telnet 或 HTTP 方式进行管理了，但有些交换机不支持 HTTP 管理方式。

学习活动 2　交换机的基本配置

交换机的简单配置是指对新购置的交换机进行的基本设置，主要包括交换机的设备命名、时间设置、密码设置、IP 地址配置、默认网关和远程管理配置等。

学习情境

网络管理员通过 Console 口进入交换机后，准备对交换机进行基本的设置。

情境分析

当交换机有一些没用的设置时，需要清空配置，恢复到刚刚出厂的状态，让交换机的配置成为一张“白纸”，这样就能按照自己的思路进行基本配置了，也能更清楚地了解配置是否生效，是否正确。本学习活动包括交换机几种配置模式的进入与退出、进入特权模式密码、交换机命名、清空交换机配置、利用“？”帮助命令、日期时钟配置、查看 Flash 内容等。

所需设备：

（1）DCS-3950 或 DCRS-5650 交换机 1 台。

（2）PC 1 台。

（3）Console 线 1 条。

学习活动拓扑结构如图 2-1-11 所示。

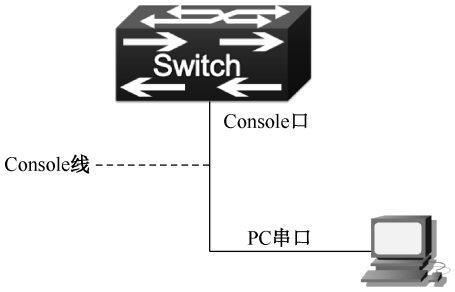


图 2-1-11　交换机基本配置

相关知识

（1）交换机出厂第一次启动，进入“ setup configuration ”，用户可以选择进入 setup 模式或者跳过 setup 模式。键入“ y ”，按【Enter】键即可进入 setup 模式。

用户在进入主菜单之前，会提示用户选择配置界面的语言种类，对英文不是很熟悉的用户可以选择“ 1 ”，进入中文提示的配置界面；选择“ 0 ”则进入英文提示的配置界面。

```
Please select language
[0]:English
[1]:中文
Selection(0|1) [0]:
```

具有中文提示的配置界面是神州数码网络产品本土化的重要特色。

（2）为了对网络进行有效的保护，允许用户以不同的身份登录交换机进行配置，允许对不同的身份设置不同的密码，不同的身份在配置交换机时有不同的权限。目前神州数码的交换机可以设置 visitor 和 admin 两种身份。

visitor 登录身份的配置权限：支持 show、ping、traceroute、clear 等命令，该身份无法进入 config 模式。admin 登录身份的配置权限是支持所有的命令。

进入特权模式命令：enable [level {visitor|admin} [<password>]]，用来指定身份及密码登录交换机。设置登录身份的相关密码：enable password level {visitor|admin}，指定登录配置模式的密码。

（3）交换机的配置模式。

① 用户模式：用户进入 CLI 界面，首先进入的就是一般用户配置模式，提示符为“ switch> ”，符号“ > ”为一般用户配置模式的提示符。当用户从特权用户配置模式使用命令 exit 退出时，可以回到一般用户配置模式。用户在一般用户配置模式下不能对交换机进行任何配置，只能查询交换机基本信息。

② 特权模式：在一般用户配置模式使用 enable 命令，如果已经配置了进入特权用户的口令，则输入相应的特权用户口令，即可进入特权用户配置模式“ switch# ”。当用户从全局配置模式使用 exit 命令退出时，也可以回到特权用户配置模式。

在特权用户配置模式下，用户可以查询交换机配置信息、各个端口的连接情况、收发数据统计等。进入特权用户配置模式后，可以用全局配置模式对交换机的各项配置进行修改，因此进行特权用户配置模式必须设置特权用户口令，防止非特权用户的非法使用，对交换机

配置进行恶意修改，造成不必要的损失。

③ 全局模式：进入特权用户配置模式后，只需使用命令 config，即可进入全局配置模式——“ switch(config)# ”。当用户在其他配置模式，如接口配置模式、VLAN 配置模式时，可以使用命令 exit 回到全局配置模式。

（4）交换机 CLI 其他使用方式。

① CLI 快捷键。【Backspace】键删除光标所在位置的前一个字符；上光标键【↑】显示上一个输入命令，最多可显示最近输入的十个命令；下光标键【↓】显示下一个输入命令，当使用上光标键回溯到以前输入的命令时，也可以使用下光标键后退；左光标键【←】为光标向左移动一个位置；右光标键【→】为光标向右移动一个位置，左右键的配合使用可对已输入的命令做覆盖修改。

```
a.【Ctrl+Z】组合键从其他配置模式（一般用户配置模式除外）直接退回到特权用户模式。
b.【Ctrl+C】组合键打断交换机ping或其他正在执行的命令进程。
c.当输入的字符串可以无冲突地表示命令或关键字时，可以使用【Tab】键将其补充成完整的命令或关键字。
d.//执行上上一级目录的命令。
```

② CLI 帮助功能。在任一命令模式下，输入“ ？ ”，获取该命令模式下的所有命令及其简单描述。在命令的关键字后，输入以空格分隔的“ ？ ”，若该位置是参数，则会输出该参数类型、范围等描述；若该位置是关键字，则列出关键字的集合及其简单描述；若输出“ <cr> ”，则此命令已输入完整，在该处按【Enter】键即可。在字符串后紧接着输入“ ？ ”，会列出以该字符串开头的所有命令。

③ CLI 对输入的检查。通过键盘输入的所有命令都要经过 Shell 检查，正确地输入命令，且执行成功，不会显示任何信息。

④ 常见错误返回信息。

```
Unrecognized command or illegal parameter!
```

命令不存在，或者参数的范围、类型、格式有错误。

```
Ambiguous command
```

根据已有输入可以产生至少两种不同的解释。

```
Invalid command or parameter
```

命令解析成功，但没有任何有效的参数记录。

```
This command is not exist in current  mode
```

命令可解析，但当前模式下不能配置该命令。

（5）CLI 支持不完全匹配。绝大部分交换机的 Shell 支持不完全匹配的搜索命令和关键字，当输入无冲突的命令或关键字时，Shell 就会正确解析。

例如，对特权用户配置命令“ show interface ethernet 1 ”只要输入“ sh in e 1 ”即可。

步骤实现

步骤 1：按照图 2-1-11 连接网络拓扑结构。

步骤 2：清空交换机的配置。

```
switch>enable                                    ! 进入特权配置模式
switch#set default                               ! 恢复出厂设置
```

```
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 3：为交换机设置 enable 密码。

```
switch>enable
switch#config                                          !进入全局配置模式
switch(config)#enable password level admin             !配置admin级别密码
Current password:                                      !原密码为空，直接按【Enter】键
New password:*****                                     !输入密码
Confirm new password:*****                             !重新输入密码，确定密码的设置
switch(config)#exit
switch#write
```

步骤 4：使用 show flash 命令查看配置文件。

```
switch#show flash
file name          file length
nos.img           1720035 bytes          ! 交换机软件系统
startup-config      0 bytes              ! 启动配置文件
running-config     783 bytes             ! 当前配置文件
switch#
```

步骤 5：设置交换机系统日期和时钟。

```
switch#clock set ?                                     ! 使用"?"查询命令格式
<HH:MM:SS>      --Time
switch#clock set 15:29:50                              ! 配置当前时间
Current time is MON JAN 01 15:29:50 2010               ! 配置完即可显示时间
switch#clock set 15:29:50 ?                            ! 使用"?"查询，原来命令没有结束
<YYYY:MM:DD>    --Date <year:2000-2035>
switch# clock set 15:29:50 2010.01.16                  ! 配置当前年月日
```

步骤 6：设置交换机名称。

```
switch(config)#hostname DCS-3950-BD1       ! 配置交换机名称
```

步骤 7：配置显示的帮助信息的语言类型。

```
DCS-3950-BD1#language ?                                !使用"?"查询帮助信息的语言类型
chinese         --Chinese
english         -- English
DCS-3950-BD1#language chinese                          !设置帮助信息语言类型为中文
DCS-3950-BD1#language ?                                !验证查询帮助信息的语言类型
chinese         --汉语
english         --英语
```

知识拓展

交换机是基于端口运行和工作的网络设备。通常，交换机拥有许多端口，有些端口用来接入公网，有些端口用来接入内网计算机。

交换机的端口可以进行带宽和工作模式的限制，一般有 force10-full、force10-half、force100-full、force100-half、force1g-full、force1g-half 和 Auto（自协商）。设置的方法很简单，使用 speed-duplex 命令即可实现。

交换机是工作在数据链路层的设备，当交换机的端口接入网络设备（如计算机）时，交换机会自动生成 MAC 地址表，查看交换机的 MAC 地址表在特权配置模式下进行，命令为 show mac-address-table。

1. 配置端口带宽限制

```
DCRS-5650-28(Config-If-Ethernet0/0/1)#speed-duplex  ?
  auto            自协商
  force10-full    10兆全双工
  force10-half    10兆半双工
  force100-full   100兆全双工
  force100-half   100兆半双工
  force1g-full    1000兆全双工
  force1g-half    1000兆半双工
DCRS-5650-28(Config-If-Ethernet0/0/1)#speed-duplex  force100-full
DCRS-5650-28(Config-If-Ethernet0/0/1)#exit
DCRS-5650-28(config)#
```

2. 管理 MAC 地址表

```
DCRS-5650-28#show mac-address-table
Read mac address table....
Vlan Mac Address               Type    Creator   Ports
---- ------------------------- ------- ---------------------------------
1    00-03-0f-26-68-35          STATIC  cluster  CPU
1    a4-1f-72-85-97-54          DYNAMIC Hardware Ethernet0/0/3
```

学习小结

本学习活动介绍了交换机的基本配置，需要注意的是，交换机的接口 IP 通过配置 VLAN 的 IP 地址来实现，交换机的帮助信息可以设置为中文。交换机端口的带宽和工作模式一般不设置，使用 Auto 模式即可。

学习活动 3　交换机文件的保存和备份

学习情境

某公司的管理员对公司的交换机进行了完整的配置后，可以让公司的网络正常工作了，现在管理员想对交换机的文件进行保存和备份。

情境分析

管理员将公司交换机的配置完成后，必须要进行保存和备份，这是管理员的重要一个工作之一。当日后交换机文件损坏时，方便快速地对文件进行恢复。

所需设备：

（1）DCS-3950 交换机 1 台。

（2）PC 1 台、TFTP Server 1 台（1 台 PC 也可以，既作为调试机又作为 TFTP 服务器）。

（3）Console 线 1 条。

（4）直通线 1 条。

学习活动拓扑结构如图 2-1-12 所示。

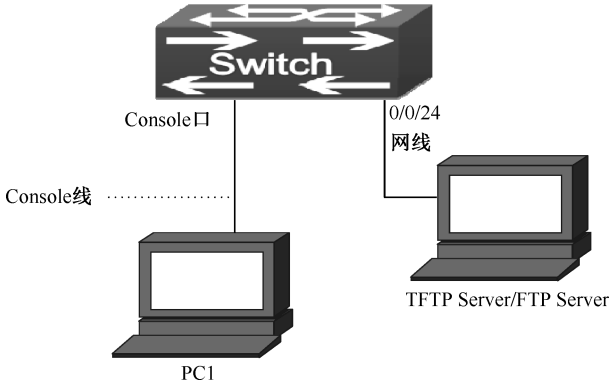


图 2-1-12　交换机文件备份拓扑结构

相关知识

交换机的文件保存在特权模式下，使用“ copy running-config startup-config ”或“ write ”命令就可以对文件进行保存。

running-config 文件保存在 DDR RAM 中，断电会消失，相当于计算机的内存。

startup-config 文件保存在 Flash 中，断电后依然存在，相当于计算机的硬盘。

可以将 startup-config 的文件，经过 TFTP（Trivial File Transfer Protocol，简单文件传输协议）软件备份到计算机中，以便下次交换机出现故障时直接恢复。

交换机的系统文件存储在 Flash 中，如果 Flash 中的配置文件遭到了破坏，交换机将无法正常工作，可以通过 TFTP 软件进行恢复，即从备份的交换机 Flash 文件或互联网下载相关版本的系统文件写到交换机中。如果系统文件没有损坏，而交换机的文件丢失了，则直接恢复文件即可。

TFTP 是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务，端口号为 69。

步骤实现

1. 交换机的保存

使用的命令如下：

```
Switch#write
Switch#%Jan 01 00:06:40 2006 Write configuration success!
```

或

```
Switch#copy running-config startup-config
Switch#%Jan 01 00:07:21 2006 Write configuration success!
```

2. 交换机配置文件的备份

步骤 1：按照图 2-1-12 连接网络拓扑结构。

步骤 2：PC 网卡的 IP 地址为 192.168.1.101/24，此处略。

步骤 3：配置 TFTP 服务器，如图 2-1-13 所示。

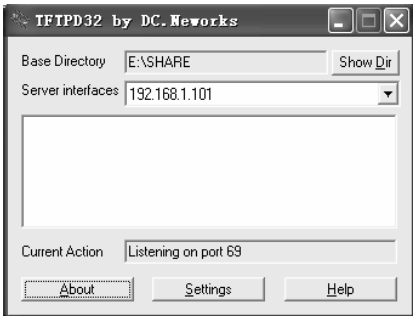


图 2-1-13　配置 TFTP 服务器

步骤 4：为交换机设置 IP 地址，验证主机与交换机是否连通。

```
switch(config)#interface vlan 1                    ！进入VLAN1的接口
switch(Config-if-Vlan1)#ip address 192.168.1.100 255.255.255.0
                                                   ！配置VLAN1的IP地址
Switch(Config-if-Vlan1)#no shutdown                ！开启该接口
Switch(Config-if-Vlan1)#exit
switch#ping 192.168.1.101                          ！测试ping通
```

步骤 5：备份配置文件。

```
switch#copy startup-config  tftp://192.168.1.101/startup_20100101
                          ！通过TFTP备份配置文件，文件名为startup_20100101
Confirm [Y/N]:y
begin to send file,wait.....
file transfers complete.
Close tftp client.
switch#
```

步骤 6：对当前的配置做修改并保存。

```
switch#config
switch(config)#hostname DCS-3950                   ！交换机命名为DCS-3950
DCS-3950(config)#exit
```

```
DCS-3950#write                                          ！保存配置
DCS-3950#
```

步骤 7：下载配置文件。

```
DCS-3950 #copy tftp://192.168.1.101/startup 20100101 startup-config
                    ！通过TFTP下载配置文件，文件名为startup_20100101
Confirm [Y/N]:y
begin to send file,wait.....
recv 865
write ok
transfer complete
close tftp client
```

步骤 8：重新启动并验证是否已经还原配置。

```
DCS-3950#reload     ！重启交换机
```

知识拓展

交换机系统升级所需设备如下：

（1）DCS-3950 交换机 1 台。

（2）PC 1 台、TFTP Server 1 台（1 台 PC 也可以，既作为调试机又作为 TFTP 服务器）。

（3）Console 线 1 条。

（4）直通线 1 条。

实验拓扑如图 2-1-14 所示。

步骤 1：按照图 2-1-14 连接网络拓扑结构。

步骤 2：配置 PC 网卡的 IP 地址为 192.168.1.101/24，此处略。

步骤 3：配置 TFTP 服务器，如图 2-1-15 所示。

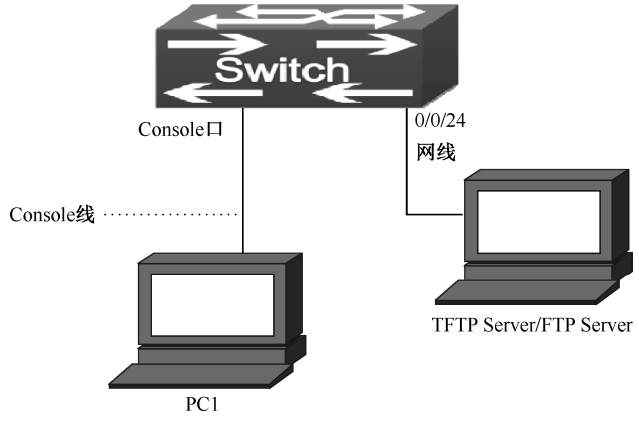


图 2-1-14　交换机文件备份拓扑

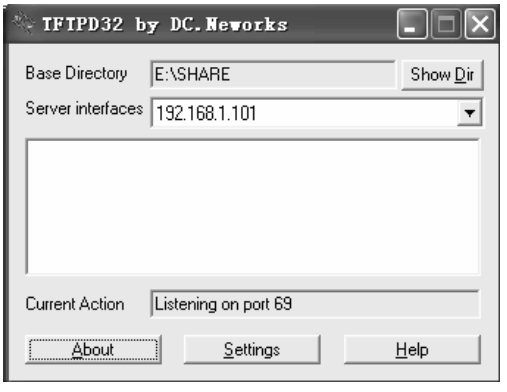


图 2-1-15　配置 TFTP 服务器

步骤 4：为交换机设置 IP 地址，验证主机与交换机是否连通。

```
switch(config)#interface vlan 1                         ！进入VLAN1的接口
switch(Config-if-Vlan1)#ip address 192.168.1.100 255.255.255.0
                                                        ！配置VLAN1的IP地址
```

```
Switch(Config-if-Vlan1)#no shutdown              ！开启该接口
Switch(Config-if-Vlan1)#exit
switch#ping 192.168.1.101                        ！测试ping通
```

步骤 5：通过 TFTP 服务器升级系统。

```
DCS-3950#copy tftp:// 192.168.1.101/nos.img nos.img
！通过TFTP将nos.img交换机软件系统上传到交换机，并且命名为nos.img
Confirm [Y/N]:y
begin to send file,wait.....
############################################################
############################################################
#########################
Recv 3330245
Begin writing flash.
End writing flash.
Write ok
transfers complete.
Close tftp client.
DCS-3950#reload       ！重启交换机
```

小贴士

（1）copy 命令中，startup-config 文件名要键入全称。

（2）Tftpd32.exe 和 Cisco TFTP Server 只支持 TFTP，不支持 FTP。

（3）如果 TFTP 和交换机之间 ping 不通，需要检查 TFTP 服务器防火墙是否开启。

（4）nos.img 是交换机系统的映像文件，保存在 Flash 中，默认文件名为 nos.img。

学习小结

本学习活动介绍了交换机文件的保存和备份，这对管理员来说是至关重要的，在备份时要注意保存的文件名和保存位置。

学习任务 2　交换机的 VLAN 配置

VLAN（Virtual Local Area Network，虚拟局域网）技术在局域网互连时得到了广泛推广和应用。VLAN 是指一个在物理网络上根据用途、工作组、应用等来逻辑划分的局域网络，是一个广播域，与用户的物理位置没有关系。VLAN 中的网络用户是通过 LAN 交换机来通信的。一个 VLAN 中的成员看不到另一个 VLAN 中的成员。

因此，划分 VLAN 能有效地控制网络广播风暴，提高网络的安全可靠性，是有效的网络监控、数据流量控制的手段，还能实现不同地理位置的部门间的局域网通信，有效地节省构建网络时所需网络设备的费用。

本学习任务分为以下三个学习活动学习

学习活动 1　交换机的 VLAN 划分。

学习活动 2　交换机间相同 VLAN 的通信。

学习活动 3　利用 SVI 实现 VLAN 间路由。

学习活动 1　交换机的 VLAN 划分

逻辑上把网络资源和网络用户按照一定的原则划分出来，把一个物理上的网络分成多个小的逻辑网络，这些逻辑网络就是 VLAN。接入层交换机上的 VLAN 划分，可以使一个交换机划分为多个 VLAN，从而保证各部门间的安全通信。

学习情境

某公司有两个部门，一个是财务部，一个是市场部，两个部门的信息端口都连接在一台交换机上。公司已经为部门分配了固定的 IP 地址段，经理想实现两个部门的相对独立，让公司的网络管理员想办法来解决。

情境分析

为了保证两个部门的相对独立，就需要划分对应的 VLAN，使交换机某些端口属于财务部，某些端口属于市场部，这样就能保证它们之间的数据互不干扰，也不影响各自的通信效率。

所需设备：

（1）DCS-3950 交换机 1 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）直通线 2 条。

学习活动拓扑结构如图 2-2-1 所示。

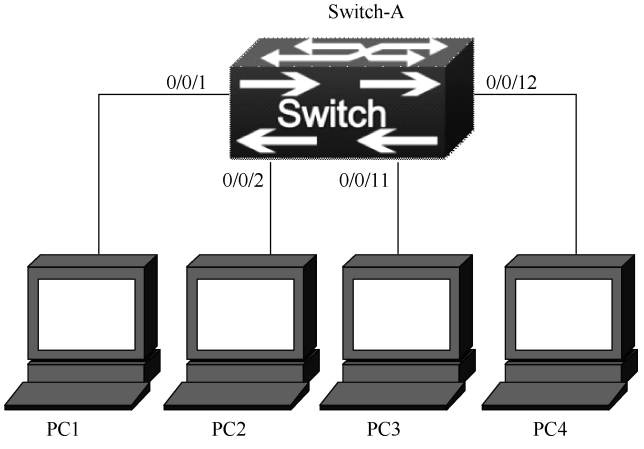


图 2-2-1　交换机 VLAN 划分拓扑结构

配置见表 2-2-1。

表 2-2-1　交换机 VLAN 划分

设　　备	端口成员	IP 地址	子网掩码
Switch 的 VLAN 10	1～10		
Switch 的 VLAN 20	11～20		
PC1	E0/0/1	192.168.1.101	255.255.255.0
PC2	E0/0/2	192.168.1.102	255.255.255.0
PC3	E0/0/11	192.168.1.103	255.255.255.0
PC4	E0/0/12	192.168.1.104	255.255.255.0

小贴士

二层交换机同一 VLAN 中的端口能互相通信，不同 VLAN 中的端口不能互相通信。二层交换机不具备路由功能。

而在三层交换机中不同 VLAN 中的端口能互相通信，因为三层交换机具备路由功能。

相关知识

1．什么是 VLAN 技术

在理解什么是 VLAN 技术前，我们需要明白广播域和冲突域这两个概念。广播域是局域网中设备之间发送广播帧的区域，即一台计算机发送广播帧的最远范围，广播存在所有局域网中，如果不进行适当的控制，广播便会充斥整个网络，产生较大的网络通信流量，消耗带宽，但广播是不可避免的，交换机对所有的广播进行转发，而路由器不会。图 2-2-2 所示为交换机广播域的形成。一个局域网中的所有设备都连接在一个共享的物理介质上，当两个接入网络的设备同时向介质发送数据时，就会发生冲突，所有设备发生冲突的最大范围就是冲突域，图 2-2-3 所示为交换机冲突域的形成。

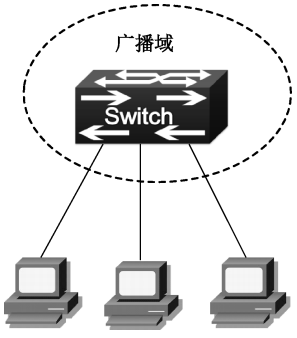


图 2-2-2　交换机广播域

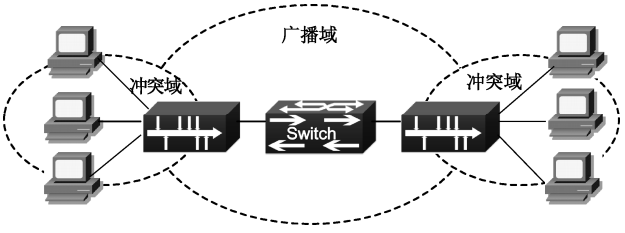


图 2-2-3　交换机广播域和冲突域

交换机提供了将大冲突域划分为小冲突域的技术：VLAN 技术。VLAN 是在一个物理网络上划分出来的逻辑网络。VLAN 技术根据功能、应用等因素，将用户从逻辑上划分为一个个功能相对独立的工作组，网络中的每台主机连接在一台交换机的端口上，并属于一个 VLAN。VLAN 的划分不受连接设备的实际物理位置的限制，如果一台主机想要同它不在同

一 VLAN 的主机通信，则必须使用第三层设备：也就是需要使用 IP 地址来通信，这就意味着不同 VLAN 中的设备之间的通信，需要通过路由器或者三层设备来实现转发。总之，VLAN 技术增加了网络连接的灵活性，控制了网络上的广播，增加了网络的安全性。

2．VLAN 操作的基本命令详解

（1）VLAN 的创建与删除。

```
vlan <vlan-id>
no vlan <vlan-id>
```

功能：创建 VLAN 并且进入 VLAN 配置模式，在 VLAN 模式中，用户可以配置 VLAN 名称并为该 VLAN 分配交换机端口，本命令的 no 操作作用为删除指定的 VLAN。

参数：<vlan-id>为要创建/删除的 VLAN 的 ID，取值为 1～4094。

命令模式：全局配置模式。

默认情况：交换机默认只有 VLAN1。

使用指南：VLAN1 为交换机的默认 VLAN，用户不能配置和删除 VLAN1，允许配置 VLAN 的总共数量为 4094 个。

举例：创建 VLAN100，并且进入 VLAN100 的配置模式。

```
switch(config)#vlan 100
switch(Config-Vlan100)#
```

（2）为 VLAN 分配交换机端口。

```
switchport interface [ethernet|portchannel] <interface-name|interface- list>]
no switchport interface [ethernet|portchannel] <interface-name|interface- list>]
```

功能：为 VLAN 分配以太网端口的命令，本命令的“ no ”操作作用为删除指定 VLAN 内的一个或一组端口。

参数：ethernet 为要添加的以太网端口，portchannel 为要添加的一个链路聚合端口，interface-name 为端口名称，如 e0/0/1，若选择端口名称则不用选择 ethernet 或 portchannel，<interface-list>为要添加或者删除的以太网端口的列表，支持“ ; ”、“ - ”，如 ethernet0/0/1;3;4-7;8，<interface-list>也可以为要添加或删除的端口链路聚合，如 port-channel 1。

命令模式：VLAN 配置模式。

默认情况：新建立的 VLAN 默认不包含任何端口。

使用指南：Access 端口为普通端口，可以加入 VLAN，但同时只允许加入一个 VLAN。

举例：为 VLAN100 分配百兆以太网端口 1，3，4～7，8。

```
switch(Config-Vlan100)#switchport interface ethernet 0/0/1;3;4-7;8
```

步骤实现

步骤 1：按照图 2-2-1 连接网络拓扑结构。

步骤 2：按照表 2-2-1 配置计算机的 IP 地址和子网掩码。

步骤 3：交换机恢复出厂设置。

```
switch>enable                                    ! 进入特权配置模式
switch#set default                               ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
```

```
switch#reload                                          ！重启交换机
Process with reboot? [Y/N]y
```

步骤 4：给交换机设置 IP 地址，即管理 IP 地址。

```
switch#config
switch(config)#interface vlan 1          ！进入VLAN1的接口
switch(Config-if-Vlan1)#ip address 192.168.1.11  255.255.255.0
                                         ！配置VLAN1的IP地址
switch(Config-if-Vlan1)#no shutdown      ！开启该端口
switch(Config-if-Vlan1)#exit
switch(config)#exit
```

步骤 5：在交换机上创建 VLAN10 和 VLAN20，并将端口 e0/0/1～10 放入 VLAN10，将端口 e0/0/11～20 放入 VLAN20。

```
Switch-A(config)#vlan 10                          ！创建VLAN10
Switch-A(config-vlan10)#switchport interface e0/0/1-10
Set the port Ethernet0/0/1 access vlan 10 successfully
Set the port Ethernet0/0/2 access vlan 10 successfully
Set the port Ethernet0/0/3 access vlan 10 successfully
Set the port Ethernet0/0/4 access vlan 10 successfully
Set the port Ethernet0/0/5 access vlan 10 successfully
Set the port Ethernet0/0/6 access vlan 10 successfully
Set the port Ethernet0/0/7 access vlan 10 successfully
Set the port Ethernet0/0/8 access vlan 10 successfully
Set the port Ethernet0/0/9 access vlan 10 successfully
Set the port Ethernet0/0/10 access vlan 10 successfully
Switch-A(Config-Vlan10)#exit
Switch-A(config)#vlan 20
Switch-A(config-vlan20)#switchport interface e0/0/11-20
Set the port Ethernet0/0/11 access vlan 20 successfully
Set the port Ethernet0/0/12 access vlan 20 successfully
Set the port Ethernet0/0/13 access vlan 20 successfully
Set the port Ethernet0/0/14 access vlan 20 successfully
Set the port Ethernet0/0/15 access vlan 20 successfully
Set the port Ethernet0/0/16 access vlan 20 successfully
Set the port Ethernet0/0/17 access vlan 20 successfully
Set the port Ethernet0/0/18 access vlan 20 successfully
Set the port Ethernet0/0/19 access vlan 20 successfully
Set the port Ethernet0/0/20 access vlan 20 successfully
Switch-A(config-vlan20)
Switch-A(config)#
```

步骤 6：查看交换机的 VLAN 划分情况。

```
Switch-A#show vlan
VLAN Name       Type      Media    Ports
---- ------------ ---------- --------- ---------------------------------------
1   default    Static   ENET    Ethernet0/0/21      Ethernet0/0/22
```

```
                                  Ethernet0/0/23      Ethernet0/0/24
                                  Ethernet0/0/25      Ethernet0/0/26
10   VLAN0010  Static   ENET     Ethernet0/0/1       Ethernet0/0/2
                                  Ethernet0/0/3       Ethernet0/0/4
                                  Ethernet0/0/5       Ethernet0/0/6
                                  Ethernet0/0/7       Ethernet0/0/8
                                  Ethernet0/0/9       Ethernet0/0/10
20   VLAN0020  Static   ENET     Ethernet0/0/11      Ethernet0/0/12
                                  Ethernet0/0/13      Ethernet0/0/14
                                  Ethernet0/0/15      Ethernet0/0/16
                                  Ethernet0/0/17      Ethernet0/0/18
                                  Ethernet0/0/19      Ethernet0/0/20
Switch-A#
```

步骤 7：测试网络的连通性。

（1）在 PC1 上 ping PC2 的 IP 地址 192.168.1.102，可以连通，说明同一 VLAN 中的计算机能互相通信，如图 2-2-4 所示。

图 2-2-4　连通性测试效果图（一）

（2）在 PC1 上 ping PC3 的 IP 地址 192.168.1.103，网络无法连通，说明不同 VLAN 中的计算机不能互相通信，如图 2-2-5 所示。

图 2-2-5　连通性测试效果图（二）

小贴士

（1）默认情况下，交换机所有端口都属于 VLAN1，因此我们通常把 VLAN1 作为交换机的管理 VLAN，因此 VLAN1 接口的 IP 地址就是交换机的管理地址。

（2）在 DCS-3950 中，一个普通端口只属于一个 VLAN。

（3）基于端口划分 VLAN，就是按交换机端口定义 VLAN 成员，每个交换机端口属于一个 VLAN。它由网络管理员静态指定 VLAN 到交换机的端口，这些连接端口会维持指定的 VLAN 设置，直到管理员重新改变它。这种方法又称为静态 VLAN，是一种最通用的 VLAN 划分方法。

（4）基于 MAC 地址划分 VLAN 指按每个连接到交换机设备的 MAC 地址定义 VLAN 成员。由于它可以按终端用户划分 VLAN，所以又常把它称为基于用户的 VLAN 划分方法。这种划分方法常需要一个保存 VLAN 管理数据库的 VLAN 配置服务器，动态地设定连接端口和对应的 VLAN 设置。在动态 VLAN 划分中，交换机端口可以自动设置 VLAN。在使用基于 MAC 地址划分 VLAN 时，一个交换机端口有可能属于多个 VLAN。

知识拓展

交换机的端口有两种模式，分别为 Access（普通模式）和 Trunk（中继模式）。在 Access 模式下，端口用于连接计算机；在 Trunk 模式下，端口用于交换机间的连接。如果交换机划分了多个 VLAN，那么 Access 模式的端口只能在某个 VLAN 中通信，而 Trunk 模式的端口则可以属于任何一个 VLAN 中。

1. 设置交换机端口类型

```
switchport mode {trunk|access}
```

功能：设置交换机的端口为 Access 模式或者 Trunk 模式。

参数：trunk 表示端口允许通过多个 VLAN 的流量，Access 为端口只能属于一个 VLAN。

命令模式：端口配置模式。

默认情况：端口默认为 Access 模式。

使用指南：工作在 Trunk 模式下的端口称为 Trunk 端口，Trunk 端口可以通过多个 VLAN 的流量，通过 Trunk 端口之间的互连，可以实现不同交换机上的相同 VLAN 的互通，工作在 Access 模式下的端口称为 Access 端口，Access 端口可以分配给一个 VLAN，并且只能分配给一个 VLAN。

举例：将端口 5 设置为 Trunk 模式，端口 8 设置为 Access 模式。

```
switch(config)#interface ethernet 0/0/5
switch(Config-If-Ethernet0/0/5)#switchport mode trunk
switch(config)#interface ethernet 0/0/8
switch(Config-If-Ethernet0/0/8)#switchport mode access
```

2. 设置 Trunk 端口

```
switchport trunk allowed vlan {<vlan-list>|all}
no switchport trunk allowed vlan
```

功能：设置 trunk 端口允许通过 VLAN，本命令的“ no ”操作作用为恢复默认情况。

参数：<vlan-list>为允许在该 Trunk 端口上通过的 VLAN 列表, all 关键字表示允许该 Trunk 端口通过所有 VLAN 的流量。

命令模式：端口配置模式。

默认情况：Trunk 端口默认允许通过所有 VLAN 的流量。

使用指南：用户可以通过本命令设置哪些 VLAN 的流量通过 Trunk 端口，没有包含的 VLAN 流量则被禁止。

举例：设置 Trunk 端口允许通过 VLAN1，3，5～20 的流量。

```
switch(config)#interface ethernet 0/0/5
switch(Config-If-Ethernet0/0/5)#switchport mode trunk
switch(Config-If-Ethernet0/0/5)#switchport trunk allowed vlan 1;3;5-20
```

3．设置 Access 端口

```
switchport access vlan <vlan-id>
no switchport access vlan
```

功能：将当前 Access 端口加入到指定 VLAN 中，本命令“ no ”操作作用为将当前端口从 VLAN 中删除。

参数：<vlan-id>为当前端口要加入的 VLAN 的 ID，取值为 1～4094。

命令模式：端口配置模式。

默认情况：所有端口默认属于 VLAN1。

使用指南：只有属于 Access 模式的端口才能加入到指定的 VLAN 中，并且 Access 端口只能加入到一个 VLAN 中。

举例：将某 Access 端口加入 VLAN100。

```
switch(config)#interface ethernet 0/0/8
switch(Config-If-Ethernet0/0/8)#switchport mode access
switch(Config-If-Ethernet0/0/8)#switchport access vlan 100
```

学习小结

本学习活动介绍了交换机的简单配置，对于初学者来说要多加练习，在练习时应多利用【Tab】键和中文的帮助。

学习活动 2　交换机间相同 VLAN 的通信

当网络中存在两台或两台以上的交换机，且每个交换机上均划分了相同的 VLAN 时，可以使交换机间所有相同 VLAN 中的计算机通过交换机互连的端口进行通信。

学习情境

某公司有销售部、技术部等部门，其中在不同楼层内都有销售部和技术部的员工计算机，为了使公司的管理更加安全与便捷，公司的领导想让网络管理员组建公司局域网，使各个部门内部的主机之间的业务往来可以进行通信，但基于安全方面的考虑，禁止部门之间的访问。

情境分析

通过划分 VLAN 使得销售部和技术部之间不可以自由访问，但部门内的计算机分布在不

同楼层的交换机上，又要能够互相访问，这就要使用 802.1q 进行跨交换机的相同部门的访问，也就是在两个交换机之间开启 Trunk 模式进行通信。

所需设备：

（1）DCS-3950 交换机 2 台。

（2）PC4 台。

（3）Console 线 1 条。

（4）直通网线 5 条。

学习活动拓扑结构如图 2-2-6 所示。

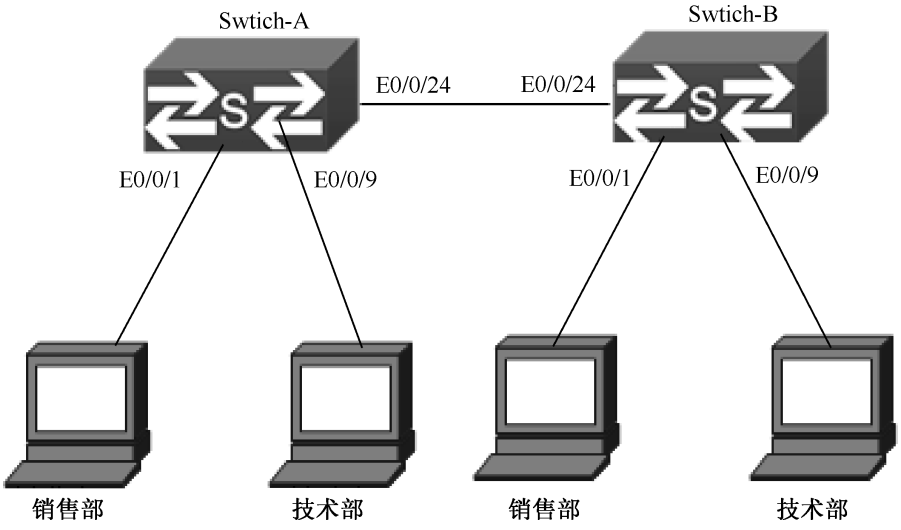


图 2-2-6　跨交换机 VLAN 通信拓扑结构

交换机 VLAN 划分见表 2-2-2。

表 2-2-2　交换机 VLAN 划分

设　　备	端口成员	IP 地址	子网掩码	备　　注
Switch-A 的 VLAN 100	1～8	无	无	无
Switch-A 的 VLAN 200	9～16	无	无	无
Switch-A	24（Trunk）	无	无	无
Switch-B 的 VLAN 100	1～8	无	无	无
Switch-B 的 VLAN 200	9～16	无	无	无
Switch-B	24 （Trunk）	无	无	无
PC1	Switch-A 的 E0/0/1	192.168.1.101	255.255.255.0	销售部
PC2	Switch-A 的 E0/0/9	192.168.1.102	255.255.255.0	技术部
PC3	Switch-B 的 E0/0/1	192.168.1.103	255.255.255.0	销售部
PC4	Switch-B 的 E0/0/9	192.168.1.104	255.255.255.0	技术部

相关知识

当网络中存在两台或两台以上的交换机，且每个交换机上均划分了相同的 VLAN 时，可

以使交换机间所有相同 VLAN 中的计算机通过交换机互连的端口进行通信。这里要学习一些新的知识，即交换机的端口模式，交换机的端口模式主要分为 Access 类型、Trunk 类型。默认情况下，交换机的端口均为 Access 类型，这种类型的端口只能隶属于一个 VLAN 中，通常用来连接计算机；而 Trunk 类型的端口可以允许多个 VLAN 通信，一般用来交换机互连。

二层交换机只有二层的功能，实现一个广播域内的主机间的通信。在 OSI 七层模型中，这个设备就工作在数据链路层。三层交换机就是在有二层的功能上通过添加一个路由模块，实现三层的路由转发功能。也就是说，三层交换机可以同时工作在数据链路层和网络层上。二层交换机同一 VLAN 中的端口能互相通信，不同 VLAN 中的端口不能互相通信。二层交换机不具备路由功能。

取消一个 VLAN 可以使用“ no vlan ”命令，取消 VLAN 的某个端口可以在 VLAN 模式下使用“ no switchport interface ethernet0/0/X ”命令，当使用“ switchport trunk allowed vlan all ”命令后，所有以后创建的 VLAN 中都会自动添加 Trunk 口为成员端口。

步骤实现

步骤 1：按照图 2-2-6 连接网络拓扑结构。

步骤 2：按照表 2-2-2 配置计算机的 IP 地址和子网掩码。

步骤 3：交换机恢复出厂设置。

```
switch>enable                                    ! 进入特权配置模式
switch#set default                               ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                    ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 4：给交换机 A 设置名称和管理地址。

```
switch(config)#hostname switch-A                 ! 交换机命名为 switch-A
switch-A(config)#interface vlan 1                ! 进入 VLAN1 的接口
switch-A(Config-if-Vlan1)#ip address 192.168.1.11  255.255.255.0
                                                 ! 配置 VLAN1 的 IP 地址
Switch-A(Config-if-Vlan1)#no shutdown            ! 开启该端口
Switch-A(Config-if-Vlan1)#exit
Switch-A(config)#
```

步骤 5：给交换机 B 设置名称和管理地址。

```
switch(config)#hostname switch-B                 ! 交换机命名为 switch-B
switch-B(config)#interface vlan 1                ! 进入 VLAN1 的接口
switch-B(Config-if-Vlan1)#ip address 192.168.1.12  255.255.255.0
                                                 ! 配置 VLAN1 的 IP 地址
Switch-B(Config-if-Vlan1)#no shutdown            ! 开启该端口
Switch-B(Config-if-Vlan1)#exit
Switch-B(config)#
```

步骤 6：在交换机 A 中创建 VLAN100 和 VLAN200，并添加端口。

```
Switch-A(config)#vlan 100                        ! 创建 VLAN100
```

```
Switch-A(config-vlan100)#switchport interface e0/0/1-8
!将 0/0/1-8 端口加入 VLAN100
Set the port Ethernet0/0/1 access vlan 100 successfully
Set the port Ethernet0/0/2 access vlan 100 successfully
Set the port Ethernet0/0/3 access vlan 100 successfully
Set the port Ethernet0/0/4 access vlan 100 successfully
Set the port Ethernet0/0/5 access vlan 100 successfully
Set the port Ethernet0/0/6 access vlan 100 successfully
Set the port Ethernet0/0/7 access vlan 100 successfully
Set the port Ethernet0/0/8 access vlan 100 successfully
Switch-A(config-vlan100)#exit
Switch-A(config)#vlan 200                    !创建 VLAN200
Switch-A(config-vlan200)#switchport interface e0/0/9-16
!将 0/0/9-16 端口加入 VLAN200
Set the port Ethernet0/0/9 access vlan 200 successfully
Set the port Ethernet0/0/10 access vlan 200 successfully
Set the port Ethernet0/0/11 access vlan 200 successfully
Set the port Ethernet0/0/12 access vlan 200 successfully
Set the port Ethernet0/0/13 access vlan 200 successfully
Set the port Ethernet0/0/14 access vlan 200 successfully
Set the port Ethernet0/0/15 access vlan 200 successfully
Set the port Ethernet0/0/16 access vlan 200 successfully
Switch-A(config-vlan200)#exit
Switch-A(config)#
```

小贴士

上述命令“0/0/1—8”中的第一个“0”表示交换机的第一个模块，第二个“0”表示交换机的第一插槽，“1—8”表示端口 1 到端口 8。

步骤 7：在交换机 B 中创建 VLAN100 和 VLAN200，并添加端口。

```
Switch-B#conf
Switch-B(config)#vlan 100                    !创建 VLAN100
Switch-B(config-vlan100)#switchport interface e0/0/1-8
!将 0/0/1-8 端口加入 VLAN100
Set the port Ethernet0/0/1 access vlan 100 successfully
Set the port Ethernet0/0/2 access vlan 100 successfully
Set the port Ethernet0/0/3 access vlan 100 successfully
Set the port Ethernet0/0/4 access vlan 100 successfully
Set the port Ethernet0/0/5 access vlan 100 successfully
Set the port Ethernet0/0/6 access vlan 100 successfully
Set the port Ethernet0/0/7 access vlan 100 successfully
Set the port Ethernet0/0/8 access vlan 100 successfully
Switch-B(config-vlan100)#exit
```

```
Switch-B(config)#vlan 200                    ！创建 VLAN200
Switch-B(config-vlan200)#switchport interface e0/0/9-16
                                             ！将 0/0/9-16 端口加入 VLAN200
Set the port Ethernet0/0/9 access vlan 200 successfully
Set the port Ethernet0/0/10 access vlan 200 successfully
Set the port Ethernet0/0/11 access vlan 200 successfully
Set the port Ethernet0/0/12 access vlan 200 successfully
Set the port Ethernet0/0/13 access vlan 200 successfully
Set the port Ethernet0/0/14 access vlan 200 successfully
Set the port Ethernet0/0/15 access vlan 200 successfully
Set the port Ethernet0/0/16 access vlan 200 successfully
Switch-B(config-vlan200)#exit
Switch-B(config)#
```

步骤 8：验证交换机 A 的 VLAN 配置。

```
Switch-A#show vlan
VLAN Name     Type    Media   Ports
----            ------------            ----------            ---------
----------------------------------------
1  default    Static    ENET      Ethernet0/0/17     Ethernet0/0/18
                                  Ethernet0/0/19     Ethernet0/0/20
                                  Ethernet0/0/21     Ethernet0/0/22
                                  Ethernet0/0/23     Ethernet0/0/24
                                  Ethernet0/0/25     Ethernet0/0/26
100   VLAN0100   Static   ENET     Ethernet0/0/1      Ethernet0/0/2
                                  Ethernet0/0/3      Ethernet0/0/4
                                  Ethernet0/0/5      Ethernet0/0/6
                                  Ethernet0/0/7      Ethernet0/0/8
200 VLAN0200   Static   ENET      Ethernet0/0/9      Ethernet0/0/10
                                  Ethernet0/0/11     Ethernet0/0/12
                                  Ethernet0/0/13     Ethernet0/0/14
                                  Ethernet0/0/15     Ethernet0/0/16
Switch-A#
```

步骤 9：验证交换机 B 的 VLAN 配置。

```
Switch-B#show vlan
VLAN Name       Type      Media    Ports
----              ------------            ----------            ---------
----------------------------------------
1  default    Static   ENET       Ethernet0/0/17     Ethernet0/0/18
                                  Ethernet0/0/19     Ethernet0/0/20
                                  Ethernet0/0/21     Ethernet0/0/22
                                  Ethernet0/0/23     Ethernet0/0/24
                                  Ethernet0/0/25     Ethernet0/0/26
100 VLAN0100   Static  ENET       Ethernet0/0/1      Ethernet0/0/2
                                  Ethernet0/0/3      Ethernet0/0/4
```

```
                                    Ethernet0/0/5       Ethernet0/0/6
                                    Ethernet0/0/7       Ethernet0/0/8
200 VLAN0200    Static    ENET      Ethernet0/0/9       Ethernet0/0/10
                                    Ethernet0/0/11      Ethernet0/0/12
                                    Ethernet0/0/13      Ethernet0/0/14
                                    Ethernet0/0/15      Ethernet0/0/16
Switch-B#
```

步骤 10：测试网络的连通性。

在 PC3 上 ping PC1 的 IP 地址 192.168.1.101，网络不连通，如图 2-2-7 所示。

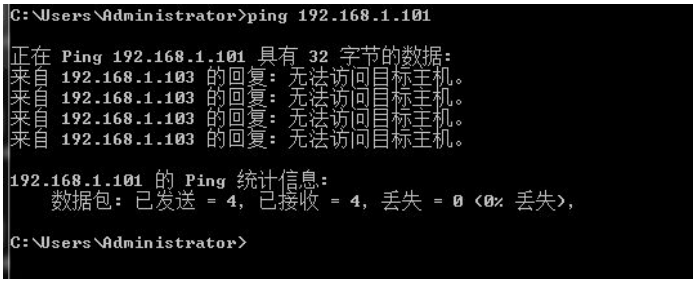


图 2-2-7　连通性测试效果图

小贴士

说明跨交换机的相同 VLAN 的计算机无法互相通信，主要原因就是没有配置 Trunk。

步骤 11：设置交换机 A 的 Trunk 端口。

```
Switch-A(config)#interface ethernet 0/0/24     ！进入端口 24
Switch-A(Config-If-Ethernet0/0/24)# switchport mode trunk
Set the port Ethernet 0/0/24 mode TRUNK successfully
                                                ！将该端口设置成 Trunk 模式
Switch-A(Config-If-Ethernet0/0/24)# switchport trunk allowed vlan all
Set the port Ethernet 0/0/24 allowed vlan successfully
                                                ！允许所有 VLAN 通过 Trunk 链路
Switch-A(Config-If-Ethernet0/0/24)#exit
```

步骤 12：设置交换机 B 的 Trunk 端口。

```
Switch-B(config)#interface ethernet 0/0/24     ！进入端口 24
Switch-B(Config-If-Ethernet0/0/24)#switchport mode trunk
Set the port Ethernet0/0/24 mode TRUNK successfully
     ！将该端口设置成 Trunk 模式
Switch-B(Config-If-Ethernet0/0/24)#switchport trunk allowed vlan all
Set the port Ethernet0/0/24 allowed vlan successfully
     ！允许所有 VLAN 通过 Trunk 链路
Switch-B(Config-If-Ethernet0/0/24)#exit
```

步骤 13：验证交换机 A 的配置。

```
Switch-A#show vlan
VLAN Name        Type      Media     Ports
```

```
----              ------------              ----------              ---------
----------------------------------------
1  default    Static   ENET         Ethernet0/0/17      Ethernet0/0/18
                                    Ethernet0/0/19      Ethernet0/0/20
                                    Ethernet0/0/21      Ethernet0/0/22
                                    Ethernet0/0/23      Ethernet0/0/24(T)
                                    Ethernet0/0/25      Ethernet0/0/26
100 VLAN0100   Static   ENET         Ethernet0/0/1       Ethernet0/0/2
                                    Ethernet0/0/3       Ethernet0/0/4
                                    Ethernet0/0/5       Ethernet0/0/6
                                    Ethernet0/0/7       Ethernet0/0/8
                                    Ethernet0/0/24(T)   !Trunk 已开
200 VLAN0200   Static   ENET         Ethernet0/0/9       Ethernet0/0/10
                                    Ethernet0/0/11      Ethernet0/0/12
                                    Ethernet0/0/13      Ethernet0/0/14
                                    Ethernet0/0/15      Ethernet0/0/16
                                    Ethernet0/0/24(T)   !Trunk 已开
Switch-A#
```

步骤 14：验证交换机 B 的配置。

```
Switch-B#show vlan
VLAN Name        Type      Media    Ports
---- ------------ ---------- --------- ----------------------------------------
1  default     Static    ENET         Ethernet0/0/17      Ethernet0/0/18
                                    Ethernet0/0/19      Ethernet0/0/20
                                    Ethernet0/0/21      Ethernet0/0/22
                                    Ethernet0/0/23      Ethernet0/0/24(T)
                                    Ethernet0/0/25      Ethernet0/0/26
100  VLAN0100    Static    ENET       Ethernet0/0/1       Ethernet0/0/2
                                    Ethernet0/0/3       Ethernet0/0/4
                                    Ethernet0/0/5       Ethernet0/0/6
                                    Ethernet0/0/7       Ethernet0/0/8
                                    Ethernet0/0/24(T)   !Trunk 已开
200  VLAN0200    Static    ENET       Ethernet0/0/9       Ethernet0/0/10
                                    Ethernet0/0/11      Ethernet0/0/12
                                    Ethernet0/0/13      Ethernet0/0/14
                                    Ethernet0/0/15      Ethernet0/0/16
                                    Ethernet0/0/24(T)   !Trunk 已开
Switch-B#
```

步骤 15：测试网络的连通性。

在 PC3 上 ping PC1 的 IP 地址 192.168.1.101，网络连通，表明交换机之前的 Trunk 链路已经成功建立，如图 2-2-8 所示。

图 2-2-8　连通性测试效果图（二）

学习小结

本学习活动介绍了跨交换机相同 VLAN 的通信，需要注意 Access 和 Trunk 端口的不同，两个交换机相连的端口同时配置了 Trunk，以保证交换机间的相同 VLAN 的通信，Trunk 端口默认允许所有 VLAN 通过。

学习活动 3　利用 SVI 实现 VLAN 间路由

通过在三层交换机上为各 VLAN 配置 SVI 口，利用三层交换机的路由功能可以实现 VLAN 间的路由。

三层交换技术就是二层交换技术加三层路由转发技术。传统的交换技术是在 OSI 网络标准模型中的第二层（即数据链路层）进行操作的，而三层交换技术是在网络模型中的第三层（即网络层）实现数据包的高速转发的。应用第三层交换技术既可实现网络路由的功能，又可以根据不同的网络状况实现最优的网络性能。

学习情境

某公司有开发部和设计部等部门，为了保证它们之间的数据互不干扰，也不影响各自的通信效率，需要划分 VLAN，使两个部门属于不同的 VLAN，但有时两个部门之间需要相互通信。

情境分析

现开发部和设计部属于不同的 VLAN，既保证两个实训室之间的数据互不干扰，又不能影响各自的通信效率，但又要使两个部门在需要的时候相互通信，此时就可以利用三层交换机来实现 VLAN 之间的通信。

所需设备：

（1）DCRS-5650 交换机 1 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）直通线 2 条。

学习活动拓扑结构如图 2-2-9 所示。

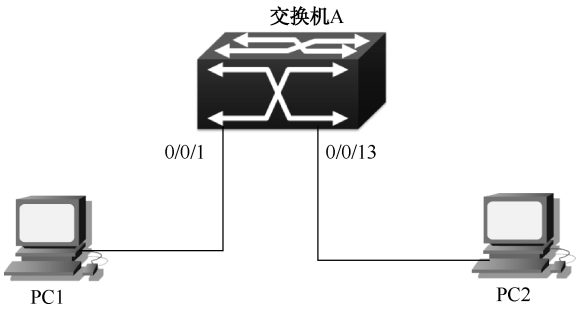


图 2-2-9　三层交换机 VLAN 路由拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 2-2-3。

表 2-2-3　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关	备　注
VLAN100	1～12	192.168.100.1	255.255.255.0	无	开发部
VLAN200	13～24	192.168.200.1	255.255.255.0	无	设计部
PC1	1～12	192.168.100.101	255.255.255.0	192.168.100.1	开发部
PC2	13～24	192.168.200.101	255.255.255.0	192.168.200.1	设计部

相关知识

三层交换机与路由器的区别：三层交换机也具有“路由”功能，它与传统路由器的路由功能总体上是一致的。虽然如此，三层交换机与路由器还是存在着相当大的本质区别的。

1. 主要功能不同

虽然三层交换机与路由器都具有路由功能，但我们不能因此而把它们等同起来，正如现在许多网络设备同时具备多种传统网络设备功能一样，例如，现在有许多宽带路由器不仅具有路由功能，还提供了交换机端口、硬件防火墙功能，但不能把它与交换机或者防火墙等同起来。因为这些路由器的主要功能还是路由功能，其他功能只不过是其附加功能，其目的是使设备适用面更广、更加实用。这里的三层交换机也一样，它仍是交换机产品，只不过它是具备了一些基本的路由功能的交换机，它的主要功能仍是数据交换。也就是说，它同时具备了数据交换和路由转发两种功能，但其主要功能还是数据交换；而路由器仅具有路由转发这一种主要功能。

2. 主要适用的环境不一样

三层交换机的路由功能通常比较简单，因为它所面对的主要是简单的局域网连接。正因如此，三层交换机的路由功能通常比较简单，路由路径远没有路由器那么复杂。它用在局域网中的主要用途还是提供快速数据交换功能，满足局域网数据交换频繁的应用特点。

而路由器则不同，它的设计初衷就是满足不同类型的网络连接，虽然也适用于局域网之间的连接，但它的路由功能更多地体现在不同类型网络之间的互连上，如局域网与广域网之间的连接、不同协议的网络之间的连接等，所以路由器主要用于不同类型的网络之间。它最

主要的功能就是路由转发，解决好各种复杂路由路径网络的连接就是它的最终目的，所以路由器的路由功能通常非常强大，不仅适用于同种协议的局域网间，也适用于不同协议的局域网与广域网间。它的优势在于选择最佳路由、负荷分担、链路备份及和其他网络进行路由信息的交换等路由器所具有的功能。为了与各种类型的网络连接，路由器的接口类型非常丰富，而三层交换机则一般仅与同类型的局域网相接，非常简单。

3．性能体现不一样

从技术上讲，路由器和三层交换机在数据包交换操作上存在着明显区别。路由器一般由基于微处理器的软件路由引擎执行数据包交换，而三层交换机通过硬件执行数据包交换。三层交换机在对第一个数据流进行路由后，它将产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层通过而不是再次路由，从而消除了路由器进行路由选择而造成的网络延迟，提高了数据包转发的效率。同时，三层交换机的路由查找是针对数据流的，它利用缓存技术，很容易利用 ASIC 技术来实现，因此，可以大大节约成本，并实现快速转发。而路由器的转发采用最长匹配的方式，实现复杂，通常使用软件来实现，转发效率较低。

正因如此，从整体性能上比较的话，三层交换机的性能要远优于路由器，非常适用于数据交换频繁的局域网中；而路由器虽然路由功能非常强大，但它的数据包转发效率远低于三层交换机，更适用于数据交换不是很频繁的不同类型网络的互连，如局域网与互联网的互连。如果把路由器，特别是高档路由器用于局域网中，则在相当大的程度上是一种浪费（就其强大的路由功能而言），而且不能很好地满足局域网通信性能需求，影响子网间的正常通信。

一个交换机虚拟接口（Switch Virtual Interface，SVI）代表一个由交换端口构成的 VLAN（其实就是通常所说的 VLAN 接口），以便于实现系统中路由和桥接的功能。一个交换机虚拟接口对应一个 VLAN，当需要路由虚拟局域网之间的流量或桥接 VLAN 之间不可路由的协议，以及提供 IP 主机到交换机的连接的时候，就需要为相应的虚拟局域网配置相应的交换机虚拟接口，其实 SVI 就是通常所说的 VLAN 接口，只不过它是虚拟的，用于连接整个 VLAN，所以通常也把这种接口称为逻辑三层接口，也是三层接口。SVI 是在 interface vlan 全局配置命令后面键入具体的 VLAN ID 时创建的。

步骤实现

步骤 1：按照图 2-2-9 连接网络拓扑结构。

步骤 2：按照表 2-2-3 配置计算机的 IP 地址和子网掩码。

步骤 3：交换机恢复出厂设置。

```
switch>enable                                          ！进入特权配置模式
switch#set default                                     ！恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ！重启交换机
Process with reboot? [Y/N]y
```

步骤 4：为交换机 A 设置主机名称和管理 IP 地址。

```
switch(config)#hostname switch-A            ！将交换机命名为switch A
```

```
switch-A(config)#interface vlan 1          ！进入VLAN1的接口
switch-A(Config-if-Vlan1)#ip address 192.168.1.11 255.255.255.0
                                           ！配置VLAN1的IP地址
Switch-A(Config-if-Vlan1)#no shutdown      ！开启该端口
Switch-A(Config-if-Vlan1)#exit
Switch-A(config)#
```

步骤 5：在交换机 A 中创建 VLAN100 和 VLAN200，并添加端口。

```
Switch-A(config)#vlan 100
Switch-A(Config-Vlan100)#switchport interface ethernet 0/0/1-12
                                  ！将e0/0/1～12端口加入VLAN100
Set the port Ethernet0/0/1 access vlan 100 successfully
Set the port Ethernet0/0/2 access vlan 100 successfully
Set the port Ethernet0/0/3 access vlan 100 successfully
Set the port Ethernet0/0/4 access vlan 100 successfully
Set the port Ethernet0/0/5 access vlan 100 successfully
Set the port Ethernet0/0/6 access vlan 100 successfully
Set the port Ethernet0/0/7 access vlan 100 successfully
Set the port Ethernet0/0/8 access vlan 100 successfully
Set the port Ethernet0/0/9 access vlan 100 successfully
Set the port Ethernet0/0/10 access vlan 100 successfully
Set the port Ethernet0/0/11 access vlan 100 successfully
Set the port Ethernet0/0/12 access vlan 100 successfully
Switch-A(Config-Vlan100)# exit
Switch-A(Config)#vlan 200
Switch-A(Config-Vlan200)#switchport interface ethernet 0/0/13-24
                                ！将e0/0/13～24端口加入VLAN200
Set the port Ethernet0/0/13 access vlan 200 successfully
Set the port Ethernet0/0/14 access vlan 200 successfully
Set the port Ethernet0/0/15 access vlan 200 successfully
Set the port Ethernet0/0/16 access vlan 200 successfully
Set the port Ethernet0/0/17 access vlan 200 successfully
Set the port Ethernet0/0/18 access vlan 200 successfully
Set the port Ethernet0/0/19 access vlan 200 successfully
Set the port Ethernet0/0/20 access vlan 200 successfully
Set the port Ethernet0/0/21 access vlan 200 successfully
Set the port Ethernet0/0/22 access vlan 200 successfully
Set the port Ethernet0/0/23 access vlan 200 successfully
Set the port Ethernet0/0/24 access vlan 200 successfully
```

步骤 6：查看交换机 A 的 VLAN 配置情况。

```
Switch-A#show vlan
VLAN Name        Type      Media     Ports
---- ------------ ---------- --------- ----------------------------------------
1    default     Static    ENET      Ethernet0/0/25     Ethernet0/0/26
                                     Ethernet0/0/27     Ethernet0/0/28
```

```
100  VLAN0100    Static    ENET     Ethernet0/0/1      Ethernet0/0/2
                                    Ethernet0/0/3      Ethernet0/0/4
                                    Ethernet0/0/5      Ethernet0/0/6
                                    Ethernet0/0/7      Ethernet0/0/8
                                    Ethernet0/0/9      Ethernet0/0/10
                                    Ethernet0/0/11     Ethernet0/0/12
200  VLAN0200    Static    ENET     Ethernet0/0/13     Ethernet0/0/14
                                    Ethernet0/0/15     Ethernet0/0/16
                                    Ethernet0/0/17     Ethernet0/0/18
                                    Ethernet0/0/19     Ethernet0/0/20
                                    Ethernet0/0/21     Ethernet0/0/22
                                    Ethernet0/0/23     Ethernet0/0/24
Switch-A#
```

步骤 7：在交换机 A 上添加 VLAN 的 IP 地址。

```
Switch-A(config)#interface vlan 100          ！进入VLAN100的接口
Switch-A(Config-if-Vlan100)#ip address  192.168.100.1  255.255.255.0
                                             ！配置VLAN100的IP地址
Switch-A(Config-if-Vlan100)#no shutdown      ！开启该端口
Switch-A(Config-if-Vlan100)#exit
Switch-A(config)#interface vlan 200          ！进入VLAN200的接口
Switch-A(Config-if-Vlan200)#ip address  192.168.200.1  255.255.255.0
                                             ！配置VLAN200的IP地址
Switch-A(Config-if-Vlan200)#no shutdown      ！开启该端口
Switch-A(Config-if-Vlan200)#exit
```

步骤 8：查看交换机 A 的 VLAN 的 IP 地址配置。

```
Switch-A#show ip int b
  Index     Interface            IP-Address       Status         Protocol
  2002      Loopback             127.0.0.1          up             up
  2004      Vlan100              192.168.100.1      up             up
  2005      Vlan200              192.168.200.1      up             up

Switch-A#
```

步骤 9：验证交换机 A 的配置。

```
Switch-A#show ip route    ！显示交换机路由信息
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.100.0/24 is directly connected, Vlan100
C       192.168.200.0/24 is directly connected, Vlan200
```

```
Total routes are : 3 item(s)
Switch-A#
```

步骤 10：测试网络的连通性。

在 PC1 上 ping PC2 的 IP 地址 192.168.200.101, 网络连通, 表明利用 SVI 可以实现 VLAN 间的路由，如图 2-2-10 所示。

图 2-2-10　连通性测试效果图

知识拓展

两台三层交换机可实现不同部门之间的网络互访。

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）PC 4 台。

（3）Console 线 1 条。

（4）直通线 5 条。

两台三层交换机 VLAN 路由拓扑结构如图 2-2-11 所示。

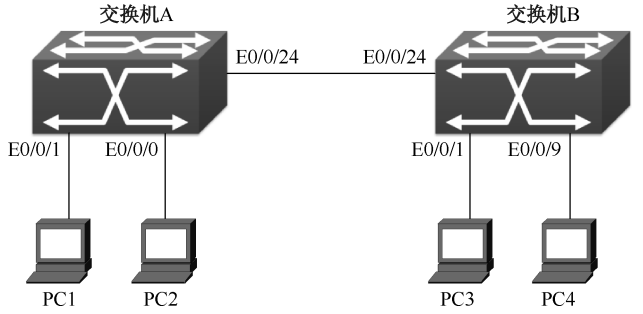


图 2-2-11　两台三层交换机 VLAN 路由拓扑结构

交换机的 VLAN 划分和 PC 的 IP 地址网络参数设置见表 2-2-4。

表 2-2-4　交换机的 VLAN 划分和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Switch-A 的 VLAN1		192.168.1.1	255.255.255.0	
Switch-A 的 VLAN100	1～8	192.168.10.1	255.255.255.0	
Switch-A 的 VLAN200	9～16	192.168.20.1	255.255.255.0	
Switch-A	0/0/24（Trunk）			

续表

设　备	端　口	IP 地址	子网掩码	网　关
Switch-B 的 VLAN1		192.168.1.11	255.255.255.0	
Switch-B 的 VLAN100	1～8	192.168.10.2	255.255.255.0	
Switch-B 的 VLAN200	9～16	192.168.20.2	255.255.255.0	
Switch-B	0/0/24（Trunk）			
PC1	Switch-A 的 0/0/1	192.168.10.101	255.255.255.0	192.168.10.1
PC2	Switch-A 的 0/0/9	192.168.20.101	255.255.255.0	192.168.20.1
PC3	Switch-B 的 0/0/1	192.168.10.102	255.255.255.0	192.168.10.2
PC4	Switch-B 的 0/0/9	192.168.20.102	255.255.255.0	192.168.20.2

步骤 1：按照图 2-2-11 连接网络拓扑结构。

步骤 2：按照表 2-2-4 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：将交换机恢复出厂设置。

```
switch#set default                          ！恢复出厂设置
switch#write                                ！保存配置
switch#reload                               ！重启交换机
```

步骤 4：为交换机 A 设置主机名称和管理 IP 地址。

```
Switch(config)#hostname Switch-A            ！交换机命名为Switch-A
Switch-A(config)#interface vlan 1           ！进入VLAN1的接口
Switch-A(Config-if-Vlan1)#ip address 192.168.1.1  255.25.255.0
                                            ！配置VLAN1的IP地址
Switch-A(Config-if-Vlan1)#no shutdown       ！开启该端口
Switch-A(Config-if-Vlan1)#exit
```

步骤 5：为交换机 B 设置主机名称和管理 IP 地址。

```
Switch(config)#hostname Switch-B            ！交换机命名为Switch-B
Switch-B(config)#interface vlan 1           ！进入VLAN1的接口
Switch-B(Config-if-Vlan1)#ip address 192.168.1.2  255.25.255.0
                                            ！配置VLAN1的IP地址
Switch-B(Config-if-Vlan1)#no shutdown       ！开启该端口
Switch-B(Config-if-Vlan1)#exit
```

步骤 6：在交换机 A 上创建 VLAN100 和 VLAN200，并添加相应端口。

```
Switch-A(config)#vlan 100                    ！创建VLAN100
Switch-A(Config-Vlan100)#switchport interface e0/0/1-8
Set the port Ethernet0/0/1 access vlan 100 successfully
Set the port Ethernet0/0/2 access vlan 100 successfully
Set the port Ethernet0/0/3 access vlan 100 successfully
Set the port Ethernet0/0/4 access vlan 100 successfully
Set the port Ethernet0/0/5 access vlan 100 successfully
Set the port Ethernet0/0/6 access vlan 100 successfully
Set the port Ethernet0/0/7 access vlan 100 successfully
Set the port Ethernet0/0/8 access vlan 100 successfully
Switch-A(Config-Vlan100)#exit
```

```
Switch-A(config)#vlan 200                    ！创建VLAN200
Switch-A(Config-Vlan200)#switchport interface e0/0/9-16
Set the port Ethernet0/0/9 access vlan 200 successfully
Set the port Ethernet0/0/10 access vlan 200 successfully
Set the port Ethernet0/0/11 access vlan 200 successfully
Set the port Ethernet0/0/12 access vlan 200 successfully
Set the port Ethernet0/0/13 access vlan 200 successfully
Set the port Ethernet0/0/14 access vlan 200 successfully
Set the port Ethernet0/0/15 access vlan 200 successfully
Set the port Ethernet0/0/16 access vlan 200 successfully
Switch-A(Config-Vlan200)#exit
Switch-A(config)#
```

步骤 7：在交换机 B 上创建 VLAN100 和 VLAN200，并添加相应端口。

```
Switch-B(config)#vlan 100                    ！创建VLAN100
Switch-B(Config-Vlan100)#switchport interface e0/0/1-8
Set the port Ethernet0/0/1 access vlan 100 successfully
Set the port Ethernet0/0/2 access vlan 100 successfully
Set the port Ethernet0/0/3 access vlan 100 successfully
Set the port Ethernet0/0/4 access vlan 100 successfully
Set the port Ethernet0/0/5 access vlan 100 successfully
Set the port Ethernet0/0/6 access vlan 100 successfully
Set the port Ethernet0/0/7 access vlan 100 successfully
Set the port Ethernet0/0/8 access vlan 100 successfully
Switch-B(Config-Vlan100)#exit
Switch-B(config)#vlan 200                    ！创建VLAN200
Switch-B(Config-Vlan200)#switchport interface e0/0/9-16
Set the port Ethernet0/0/9 access vlan 200 successfully
Set the port Ethernet0/0/10 access vlan 200 successfully
Set the port Ethernet0/0/11 access vlan 200 successfully
Set the port Ethernet0/0/12 access vlan 200 successfully
Set the port Ethernet0/0/13 access vlan 200 successfully
Set the port Ethernet0/0/14 access vlan 200 successfully
Set the port Ethernet0/0/15 access vlan 200 successfully
Set the port Ethernet0/0/16 access vlan 200 successfully
Switch-B(Config-Vlan200)#exit
Switch-B(config)#
```

步骤 8：在交换机 A 上配置 Trunk 端口。

```
Switch-A(config)#int e0/0/24                 ！进入端口24
Switch-A(Config-If-Ethernet0/0/24)#switchport mode trunk
！将该端口设置成Trunk模式
Set the port Ethernet0/0/24 mode TRUNK successfully
Switch-A(Config-If-Ethernet0/0/24)#switchport trunk allowed vlan all
set the port Ethernet0/0/24 allowed vlan successfully
Switch-A(Config-If-Ethernet0/0/24)#
```

```
Switch-A(Config-If-Ethernet0/0/24)#exit
```

步骤 9：在交换机 B 上配置 Trunk 端口。

```
Switch-B(config)#int e0/0/24                    ！进入端口24
Switch-B(Config-If-Ethernet0/0/24)#switchport mode trunk
！将该端口设置成Trunk模式
Set the port Ethernet0/0/24 mode TRUNK successfully
Switch-B(Config-If-Ethernet0/0/24)#switchport trunk allowed vlan all
set the port Ethernet0/0/24 allowed vlan successfully
Switch-B(Config-If-Ethernet0/0/24)#
Switch-B(Config-If-Ethernet0/0/24)#exit
```

步骤 10：在交换机 A 上查看 VLAN 的配置。

```
Switch-A#show vlan
VLAN Name        Type      Media     Ports
---- ------------ ---------- --------- ------------------------------------
1    default     Static    ENET      Ethernet0/0/17     Ethernet0/0/18
                                     Ethernet0/0/19     Ethernet0/0/20
                                     Ethernet0/0/21     Ethernet0/0/22
                                     Ethernet0/0/23     Ethernet0/0/24(T)
                                     Ethernet0/0/25     Ethernet0/0/26
                                     Ethernet0/0/27     Ethernet0/0/28
100  VLAN0100    Static    ENET      Ethernet0/0/1      Ethernet0/0/2
                                     Ethernet0/0/3      Ethernet0/0/4
                                     Ethernet0/0/5      Ethernet0/0/6
                                     Ethernet0/0/7      Ethernet0/0/8
                                     Ethernet0/0/24(T)
200  VLAN0200    Static    ENET      Ethernet0/0/9      Ethernet0/0/10
                                     Ethernet0/0/11     Ethernet0/0/12
                                     Ethernet0/0/13     Ethernet0/0/14
                                     Ethernet0/0/15     Ethernet0/0/16
                                     Ethernet0/0/24(T)
Switch-A#
```

步骤 11：在交换机 B 上验证其配置。

```
Switch-B#show vlan
VLAN Name        Type      Media     Ports
---- ------------ --------- --------- ------------------------------------
1    default     Static    ENET      Ethernet0/0/17     Ethernet0/0/18
                                       Ethernet0/0/19     Ethernet0/0/20
                                       Ethernet0/0/21     Ethernet0/0/22
                                       Ethernet0/0/23     Ethernet0/0/24(T)
                                       Ethernet0/0/25     Ethernet0/0/26
                                       Ethernet0/0/27     Ethernet0/0/28
100  VLAN0100    Static    ENET      Ethernet0/0/1      Ethernet0/0/2
                                       Ethernet0/0/3      Ethernet0/0/4
                                       Ethernet0/0/5      Ethernet0/0/6
```

```
                                        Ethernet0/0/7      Ethernet0/0/8
                                        Ethernet0/0/24(T)
200  VLAN0200     Static     ENET      Ethernet0/0/9      Ethernet0/0/10
                                        Ethernet0/0/11     Ethernet0/0/12
                                        Ethernet0/0/13     Ethernet0/0/14
                                        Ethernet0/0/15     Ethernet0/0/16
                                        Ethernet0/0/24(T)
Switch-B#
```

步骤 12：在交换机 A 上添加 VLAN 的地址。

```
Switch-A(config)#interface vlan 100            !进入VLAN100的接口
Switch-A(Config-if-Vlan100)#ip address 192.168.10.1  255.255.255.0
                                               !配置VLAN100的IP地址
Switch-A(Config-if-Vlan100)#no shutdown        !开启该端口
Switch-A(Config-if-Vlan100)#exit
Switch-A(config)#interface vlan 200            !进入VLAN200的接口
Switch-A(Config-if-Vlan200)#ip address 192.168.20.1 255.255.255.0
                                               !配置VLAN200的IP地址
Switch-A(Config-if-Vlan200)#no shutdown        !开启该端口
Switch-A(Config-if-Vlan200)#exit
```

步骤 13：查看交换机 A 上的 VLAN 地址。

```
Switch-A#show ip int brief
Index     Interface         IP-Address      Status          Protocol
2002      Loopback          127.0.0.1       up              up
2004      Vlan1             192.168.1.1     up              up
2005      Vlan100           192.168.10.1    up              up
2006      Vlan200           192.168.20.1    up              up

Switch-A#
```

步骤 14：在交换机 B 上添加 VLAN 的地址。

```
Switch-B(config)#interface vlan 100        !进入VLAN100的接口
Switch-B(Config-if-Vlan100)#ip address 192.168.10.2 255.255.255.0
                                           !配置VLAN100的IP地址
Switch-B(Config-if-Vlan100)#no shutdown    !开启该端口
Switch-B(Config-if-Vlan100)#exit
Switch-B(config)#interface vlan 200        !进入VLAN200的接口
Switch-B(Config-if-Vlan200)#ip address 192.168.20.2 255.255.255.0
                                           !配置VLAN200的IP地址
Switch-B(Config-if-Vlan200)#no shutdown    !开启该端口
Switch-B(Config-if-Vlan200)#exit
```

步骤 15：查看交换机 B 上的 VLAN 地址。

```
Switch-B#show ip int brief
Index     Interface           IP-Address    Status            Protocol
2002      Loopback            127.0.0.1       up                up
2004      Vlan1               192.168.1.11    up                up
```

```
2005     Vlan100            192.168.10.2    up                up
2006     Vlan200            192.168.20.2    up                up

Switch-B#
```

步骤 16：查看交换机 A 的路由表。

```
Switch-A#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      192.168.1.0/24 is directly connected, Vlan1
C      192.168.10.0/24 is directly connected, Vlan100
C      192.168.20.0/24 is directly connected, Vlan200
Total routes are : 4 item(s)
Switch-A#
```

步骤 17：查看交换机 B 的路由表。

```
Switch-B#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      192.168.1.0/24 is directly connected, Vlan1
C      192.168.10.0/24 is directly connected, Vlan100
C      192.168.20.0/24 is directly connected, Vlan200
Total routes are : 4 item(s)
Switch-B#
```

步骤 18：测试网络的连通性。

在 PC3 上 ping PC1 的 IP 地址 192.168.10.101 和 PC2 的 IP 地址 192.168.20.101，网络是连通的，表明利用 SVI 可以实现 VLAN 间的路由，如图 2-2-12 所示。

```
C:\Users\Administrator>ping 192.168.10.101

正在 Ping 192.168.10.101 具有 32 字节的数据:
来自 192.168.10.101 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.10.101 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.10.101 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.10.101 的回复: 字节=32 时间<1ms TTL=128

192.168.10.101 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 192.168.20.101

正在 Ping 192.168.20.101 具有 32 字节的数据:
来自 192.168.20.101 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.20.101 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.20.101 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.20.101 的回复: 字节=32 时间<1ms TTL=63

192.168.20.101 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```

图 2-2-12 连通性测试效果图

学习小结

本学习活动介绍了利用 SVI 实现 VLAN 之间的通信，在二层交换机上配置 VLAN 后，只能实现相同 VLAN 的通信，如果想实现 VLAN 间的通信，就必须借助于三层设备（三层交换机或路由器），路由器实现 VLAN 间通信，在后面章节中进行介绍。

学习任务 3 交换机的常用技术

交换机是一种功能非常强大、应用非常广泛的网络设备。其中，VLAN 技术是交换机最典型的应用。另外，还有链路聚合技术、生成树技术和 DHCP 技术等的应用。本学习活动重点学习交换机的三个常用技术，因此设计三个学习活动来进行学习。

学习活动 1　交换机的链路聚合技术。

学习活动 2　交换机的生成树技术。

学习活动 3　交换机的 DHCP 技术。

学习活动 1　交换机的链路聚合技术

链路聚合是将两个或更多数据信道结合成一个单个的信道，该信道以一个单个的更高带宽的逻辑链路出现。链路聚合是一种重要的技术，它用于合并带宽并且建立有恢复能力的冗余链路。

学习情境

某公司生产部门和质检部门分别使用一台交换机提供 20 多个信息点，两个部门的互通通过一根级联网线实现。每个部门的信息点都是 100Mb/s 带宽。两个部门之间的带宽也是 100Mb/s，如果部门之间需要大量传送数据，则会明显感觉带宽资源紧张。当部门之间大量用户都以 100Mb/s 传输数据的时候，部门间的链路就呈现了独木桥的状态，必然造成网络传输效率的下降等后果。

解决这个问题的办法就是提高部门之间的连接带宽，实现的办法是采用 1000Mb/s 端口替换原来的 100Mb/s 端口，但是这样无疑增加了组网的成本，需要更新端口模块，并且线缆也需要做进一步的升级。

情境分析

当采用 1000Mb/s 端口替换原来的 100Mb/s 端口进行互连时，考虑到公司成本的增加和工程的烦琐性，可将几条链路聚合，这几条链路必须同时连接在两个相同的设备之间，这样不仅增加了两个部门链路之间的带宽，也节约了公司的成本。交换机和 PC 的 IP 地址网络参数设置见表 2-3-1，如果链路聚合成功，则 PC1 可以连通 PC2。

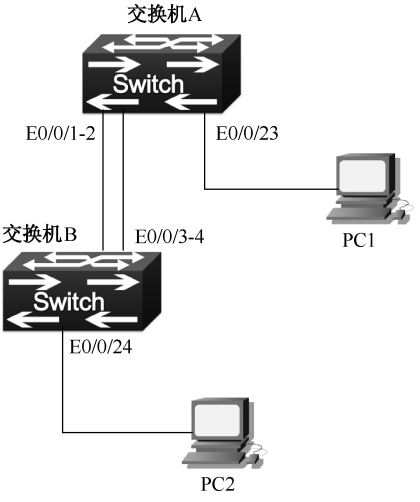


图 2-3-1　交换机链路聚合拓扑结构

所需设备：

（1）DCS-3950 交换机 2 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）直通线 4～8 条。

学习活动拓扑结构如图 2-3-1 所示。

交换机和 PC 的 IP 地址网络参数设置见表 2-3-1。

表 2-3-1　交换机和 PC 的 IP 地址网络参数设置

设　　备	IP 地址	子网掩码	端　　口
交换机 A	192.168.1.11	255.255.255.0	1 和 2　port–group
交换机 B	192.168.1.12	255.255.255.0	3 和 4　port–group
PC1	192.168.1.101	255.255.255.0	交换机 A 端口 23
PC2	192.168.1.102	255.255.255.0	交换机 B 端口 24

相关知识

（1）为使 port channel 正常工作，port channel 的成员端口必须具有以下相同的属性：端口均为全双工模式、端口速率相同、端口类型相同、端口同为 Access 端口并属于同一个 VLAN

或者同为 802.1q Trunk 端口，如果端口为 Trunk 端口，则其 allowed VLAN 和 native VLAN 属性也应该相同。

（2）支持任意两个交换机物理端口的汇聚，最大组数为 6 个，组内最多的端口数为 8 个。

（3）检查对端交换机的对应端口是否配置端口聚合组，并要查看配置方式是否相同，如果本端是手工方式，则对端也应该配置了手工方式，如果本端是 LACP 动态生成的，则对端也应该是 LACP 动态生成的，否则端口聚合组不能正常工作。还要注意，如果两端收发的都是 LACP，则至少有一端是 Active 的，否则两端都不会发起 LACP 数据报。

（4）port-group 命令详解。

```
port-group <port-group-number>[load-balance{src-mac|dst-src-mac
|src-ip|dst-ip|dst-src-ip}]
no <port-group-number>[load-balance]
```

功能：新建一个 port-group，并且设置该组的流量分担方式。如果没有指定流量分担方式，则为默认的流量分担模式。该命令的“ no ”操作功能为删除该组或者恢复该组流量分担的默认值，load-balance 表示恢复默认流量分担，否则为删除该组。

参数：<port-group-number>为 port channel 的组号，值为 1～16，如果已经存在该组号则会报错。dst-mac 根据目的 MAC 地址进行流量分担，src-mac 根据 MAC 地址进行流量分担，dst-src-mac 根据目的 MAC 地址和源 MAC 地址进行流量分担, dst-ip 根据目的 IP 地址进行流量分担，src-ip 根据源 IP 地址进行流量分担，dst-src-ip 根据目的 IP 地址和源 IP 地址进行流量分担。如果采用修改流量分担方式，并且该 port-group 已经形成一个 port-channel，则这次修改的流量分担方式只有在下次汇聚时才会生效。

命令模式：交换机全局配置模式。

默认情况：默认交换机端口不属于 port channel，不启动 LACP 协议。

举例：新建一个 port-group，并且采用默认的流量分担方式。

```
switch(config)#port-group 1
```

删除一个 port-group。

```
switch(config)#no port-group 1
```

（5）port-group mode 命令详解。

```
port-group <port-group-number> mode {active|passive|on}
no port-group <port-group-number>
```

功能：将物理端口加入 port channel，该命令的“ no ”操作功能为将端口从 port channel 中去除。

参数：<port-group-number>为 port channel 的组号，值为 1～16，active（0）启动端口的 LACP 协议，并设置为 active 模式，passive（1）启动端口的 LACP 协议，并设置为 passive 模式，on（2）强制端口加入 port channel，不启动 LACP 协议。

命令模式：交换机端口配置模式。

默认情况：默认交换机端口不属于 port channel，不启动 LACP 协议。

使用指南：如果不存在该组, 则会先建立该组, 然后将端口加入到组中。在一个 port-group 中所有的端口加入的模式必须一样, 以第一个加入该组的端口模式为准。端口以 on 模式加入一个组是强制性的，所谓强制性表示本端交换机端口聚合不依赖对端的信息，只要在组中有两个以上的端口，并且这些端口的 VLAN 信息一致，则组中的端口就能聚合成功。端口以

active 和 passive 方式加入一个组是运行 LACP 协议的，但两端必须有一个组中的端口是以 active 方式加入的，如果两端都是 passive，则端口永远无法聚合起来。

（6）show port-group 命令详解。

```
show port-group [<port-group-number>]{brief|detail|load-balance|port
|port-channel}
```

参数：<port-group-number>为要显示的 port channel 的组号，值为 1～16，brief 显示摘要信息，detail 显示详细信息，load-balance 显示流量分担信息，port 显示成员端口信息，port-channel 显示聚合端口信息。如果没有指定 port-group-number，则显示所有 port-group 的信息。

命令模式：特权配置模式。

步骤实现

步骤 1：按照图 2-3-1 连接拓扑结构。

步骤 2：按照表 2-3-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          ！进入特权配置模式
switch#set default                                     ！恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ！重启交换机
Process with reboot? [Y/N]y
```

步骤 4：为交换机 A 设置名称和管理地址。

```
switch#config
switch(config)#hostname switchA                ！交换机名称为switchA
switchA(config)#interface vlan 1               ！进入VLAN1接口
switchA(Config-if-Vlan1)#ip address 192.168.1.11  255.255.255.0
                                               ！配置VLAN1的IP地址
switchA(Config-if-Vlan1)#no shutdown           ！开启该端口
switchA(Config-if-Vlan1)#exit
switchA(config)#spanning-tree                  ！启用生成树协议
MSTP is starting now,please wait.............
MSTP is enabled successfully.
```

步骤 5：为交换机 B 设置名称和管理地址。

```
switch#config
switch(config)#hostname switchB            ！交换机名称为switchB
switchB(config)#interface vlan 1           ！进入VLAN1接口
switchB(Config-if-Vlan1)#ip address 192.168.1.12 255.255.255.0
                                           ！配置VLAN1的IP地址
switchB(Config-if-Vlan1)#no shutdown       ！开启该端口
switchB(Config-if-Vlan1)#exit
switchB(config)#spanning-tree              ！启用生成树协议
```

```
MSTP is starting now,please wait.............
MSTP is enabled successfully.
```

步骤 6：在交换机 A 上创建 port-group。

```
switchA(config)#port-group 1                    ！创建聚合端口1
switchA(config)#
```

步骤 7：在交换机 A 上验证配置。

```
switchA#show port-group brief                   ！显示port-group 1的摘要信息
Port -group number：1
Number of ports in port-group：1  Maxports in port-channel=8
Number of port-channels：0  Max port-channels：1
switchA#
```

小贴士

上述显示内容中，“Number of ports in port-group”表示在 port-group 中的端口数，“Maxports”表示组中最大允许的端口数，“Number of port-channels”表示是否已经聚合成功，“Max port-channels”表示 port-group 所能形成的最大聚合端口数。

步骤 8：在交换机 B 上创建 port-group。

```
switchB(config)#port-group 1                    ！创建聚合端口
switchB(config)#
```

步骤 9：在交换机 A 上手工生成链路聚合组。

```
switchA(config)#interface ethernet0/0/1-2
switchA(Config-If-Port-Range)#port-group 1 mode on
！强制e0/0/1和2端口加入聚合端口，并设置为on模式
switchA(Config-If-Port-Range)#exit
switchA(config)#interface port-channel 1    ！进入聚合端口
switchA(Config-If-Port-Channel1)#
```

步骤 10：在交换机 A 上验证配置。

```
switchA#show vlan
VLAN    Name        Type     Media  Ports
1       default     Static   ENET   Ethernet0/0/3    Ethernet0/0/4
                                    Ethernet0/0/5    Ethernet0/0/6
                                    Ethernet0/0/7    Ethernet0/0/8
                                    Ethernet0/0/9    Ethernet0/0/10
                                    Ethernet0/0/11   Ethernet0/0/12
                                    Ethernet0/0/13   Ethernet0/0/14
                                    Ethernet0/0/15   Ethernet0/0/16
                                    Ethernet0/0/17   Ethernet0/0/18
                                    Ethernet0/0/19   Ethernet0/0/20
                                    Ethernet0/0/21   Ethernet0/0/22
                                    Ethernet0/0/23   Ethernet0/0/24
                                     Port-Channel1
                                    ！port-channel1已经存在
```

步骤 11：在交换机 B 上手工生成链路聚合组。

```
switchB(config)#interface ethernet0/0/3-4
switchB(Config-If-Port-Range)#port-group 1 mode on
                                    ！强制e0/0/3和4端口加入聚合端口
switchB(Config-If-Port-Range)#exit
switchB(config)#interface port-channel 1   ！进入聚合端口
switchB(Config-If-Port-Channel1)#
```

步骤 12：在交换机 B 上验证配置。

```
switchB#show port-group brief              ！显示port-group摘要信息
Port-group number：1
Number of ports in port-group：1  Maxports in port-channel=8
Number of port-channels：1  Max port-channels：1
```

步骤 13：在交换机 A 上实现 LACP 动态生成链路聚合。

```
switchA(config)#interface Ethernet 0/0/1-2
switchA(Config-If-Port-Range)#port-group 1 mode active
！将e0/0/1和2端口加入聚合端口，并设置为active模式
switchA(Config-If-Port-Range)#exit
switchA(config)#interface port-channel 1       ！进入聚合端口
switchA(Config-If-Port-Channel1)#
```

步骤 14：在交换机 A 上验证配置。

```
switchA# show vlan
VLAN    Name        Type     Media   Ports
1       default     Static   ENET    Ethernet0/0/3   Ethernet0/0/4
                                        .      Ethernet0/0/5    Ethernet0/0/6
                                               Ethernet0/0/7    Ethernet0/0/8
                                               Ethernet0/0/9    Ethernet0/0/10
                                               Ethernet0/0/11   Ethernet0/0/12
                                               Ethernet0/0/13   Ethernet0/0/14
                                               Ethernet0/0/15   Ethernet0/0/16
                                               Ethernet0/0/17   Ethernet0/0/18
                                               Ethernet0/0/19   Ethernet0/0/20
                                               Ethernet0/0/21   Ethernet0/0/22
                                               Ethernet0/0/23   Ethernet0/0/24
                                               Port-Channel1
                                               ！Port-Channel1已经存在
```

步骤 15：在交换机 B 上实现 LACP 动态生成链路聚合。

```
switchB(config)#interface e0/0/3-4
switchB(Config-If-Port-Range)#port-group 1 mode passive
                              ！将e0/0/3和4端口加入聚合端口，并设置为passive模式
switchB(config)#interface port-channel 1   ！进入聚合端口
switchB(Config-If-Port-Channel1)#
```

步骤 16：在交换机 B 上验证配置。

```
switchB#show port-group brief                    ！显示port-group摘要信息
Port-group number：2
```

```
Number of ports in port-group：1  Maxports in port-channel=8
Number of port-channels：1  Max port-channels：1
```

步骤 17：使用 ping 命令验证，见表 2-3-2。

表 2-3-2　ping 命令验证

交换机 A	交换机 B	结　果	原　因
1、2	3、4	通	链路聚合组连接正确
1、2	3、4	通	拔掉交换机 B 端口 4 的网线，仍然可以连通（需要一些时间），此时用 show vlan 命令查看结果，port-channel 消失。只有一个端口连接的时候，没有必要维持一个 port-channel
1、2	5、6	通	等待一小段时间后，仍然是连通的。用 show vlan 命令查看结果，此时把两台交换机的 spanning-tree 功能禁用，这时候使用第三步和第四步的结果会不同。采用第四步的方法将会形成环路

小贴士

特别注意：将两台交换机的端口都聚合后再进行物理上的连接，否则会形成广播风暴，影响交换机的工作。

知识拓展

（1）一些命令不能在 port channel 端口使用，包括 arp、bandwidth、ip、ip-forward 等。

（2）在强制生成端口聚合组时，由于汇聚是手工配置触发的，如果 VLAN 信息不一致导致汇聚失败，则汇聚组一直会停留在没有汇聚的状态，必须通过往该 group 端口增加和删除端口来触发端口的再次汇聚，如果 VLAN 信息还不一致，则仍然不能汇聚成功。直到 VLAN 信息一致并且在增加和删除端口汇聚的情况下端口才能汇聚成功。

（3）port-channel 一旦形成，所有对于端口的设置只能在 port-channel 端口上进行。

（4）LACP 必须和 Security、802.1x 的端口互斥，如果端口已经配置了上述两种协议，就不允许被启用 LACP。

（5）interface port-channel 命令详解。

命令：interface port-channel <port-channel-number>。

功能：进入聚合端口配置模式。

命令模式：全局配置模式。

使用指南：进入聚合端口模式进行配置时，如果是对 GVRP、spanning tree、模块做配置，则对聚合端口生效；如果聚合端口不存在，即在端口没有聚合起来时先提示错误信息，记录该用户配置操作，当端口真正聚合以后恢复用户刚才对形成聚合端口的配置动作，注意只能恢复一次；如果因为某种原因聚合组被拆散后又聚合起来，则用户一开始的配置不能被恢复。如果是对其他模块做配置，如做 shutdown、speed 配置，则是对该 port-channel 对应的 port-group 中的所有成员端口生效，起到一个群配的作用。

学习小结

本学习活动介绍了交换机的链路聚合技术，在设置交换机的端口汇聚时应选择偶数数码的端口，而且选择的端口必须是连续的，端口汇聚组要设置成 Trunk 模式。

学习活动 2　交换机的生成树技术

交换机之间具有冗余链路本来是一件很好的事情，但是它有可能引起的问题比它能够解决的问题还要多。如果准备两条以上的路，就必然形成一个环路，交换机并不知道如何处理环路，只有周而复始地转发帧，形成一个“死环路”，这个死环路会造成整个网络处于阻塞状态，导致网络瘫痪。采用生成树协议可以避免环路。

学习情境

生成树协议的根本目的是将一个存在物理环路的交换网络变成一个没有环路的逻辑树形网络。IEEE 802.1d 协议通过在交换机上运行一套复杂的 STA 算法，使冗余端口置于“阻断状态”，使得接入网络的计算机在与其他计算机网络通信时，只有一条链路生效，而当这个链路出现故障无法使用时，IEEE 802.1d 协议会重新计算网络链路，将处于“阻断状态”的端口重新打开，从而既保证网络正常运转，又保证了冗余能力。

情境分析

本任务的两台交换机之间连接两根网线，默认情况下交换机所有端口属于 VLAN1，并分别在两台交换机上连接 PC1 和 PC2 做测试，当没有在交换机上启用生成树协议时，用两条网线连接两台交换机将形成广播风暴，不一会儿，交换机会出现死机情况，PC1 和 PC2 不能正常通信，因此必须在两台交换机上启用生成树协议来阻止因交换机物理环路导致的死机现象。现 IP 地址设置和网络连接分别如图 2-3-2 和表 2-3-3 所示，如果正确配置了生成树协议，则 PC1 可以连通 PC2，见表 2-3-3。

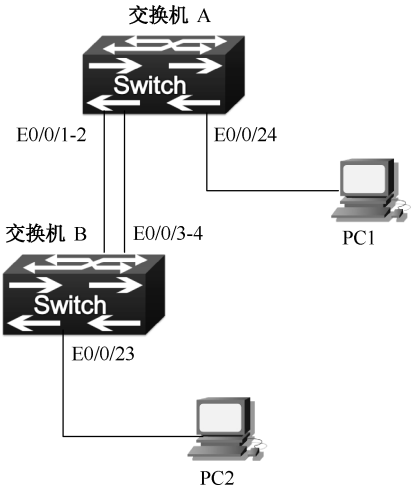


图 2-3-2　交换机生成树协议配置拓扑结构

所需准备：

（1）DCS-3950 交换机 2 台。

（2）PC 2 台。

（3）Console 线 1～2 条。

（4）直通线 4～8 条。

学习活动拓扑结构如图 2-3-2 所示。

IP 地址网络参数设置见表 2-3-3。

表 2-3-3　IP 地址网络参数设置

设　　备	IP 地址	子网掩码
交换机 A	10.1.157.100	255.255.255.0
交换机 B	10.1.157.101	255.255.255.0
PC1	10.1.157.103	255.255.255.0
PC2	10.1.157.104	255.255.255.0

相关知识

生成树协议的功能是维护一个无回路的网络，如果将网络回路中的某个端口暂时“ 阻塞 ”，到每个目的地的无回路路径就形成了，设计冗余链路的目的就是当网络发生故障（某个端口失效）时有一条后备路径替补上来。在全局模式下运行命令 spanning-tree 即启用生成树协议。命令 spanning-tree mode {mstp|stp}为设置交换机运行 spanning-tree 的模式，本命令的 no 操作是恢复交换机默认的模式，默认模式下交换机运行多生成树协议。

1．STP（生成树协议）

目的：为了防止冗余时产生环路。

原理：所有 VLAN 成员端口都加入一棵树，将备用链路的端口设为 BLOCK，直到主链路出现问题之后，BLOCK 链路才为 UP，端口的状态进行转换。

BLOCK>LISTEN>LERARN>FORWARD>DISABLE 总共经历 50s 时间，生成树协议工作时，正常情况下，交换机的端口要经过几个工作状态的转变。物理链路待接通时，将在 block 状态停留 20s，之后在 listen 状态 15s，经过 15s 的 learn，最后成为 forward 状态。

缺点：收敛速度慢，效率低。

解决收敛速度慢的补丁：POSTFACT/UPLINKFAST（检查直连链路）/BACKBONEFAST。

2．MSTP（多生成树协议）

目的：解决 STP 与 RSTP 中的效率低、占用资源的问题。

原理：部分 VLAN 为一棵树。

如果想在交换机上运行 MSTP，首先必须在全局模式下打开 MSTP 开关。在没有打开全局 MSTP 开关之前，打开端口的 MSTP 开关是不允许的。MSTP 定时器参数之间是有相关性的，错误配置可能导致交换机不能正常工作。用户在修改 MSTP 参数时，应该清楚所产生的各个拓扑。除了全局的基于网桥的参数配置外，其他的是基于各个实例的配置，在配置时一定要注意。

步骤实现

步骤 1：按照图 2-3-2 正确连接拓扑结构。

步骤 2：按照表 2-3-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：将交换机恢复出厂设置。

```
switch#set default                          ！恢复出厂设置
switch#write                                ！保存配置
switch#reload                               ！重启交换机
```

步骤 4：为交换机 A 设置名称和管理地址。

```
switch#config
switch(config)#hostname switchA             ！将交换机命名为switchA
switchA(config)#interface vlan 1            ！进入VLAN1的接口
switchA(Config-if-Vlan1)#ip address 10.1.157.100 255.25.255.0
                                            ！配置VLAN1的IP地址
switchA(Config-if-Vlan1)#no shutdown        ！开启该端口
switchA(Config-if-Vlan1)#exit
switchA(config)#
```

步骤 5：为交换机 B 设置名称和管理地址。

```
switch#config
switch(config)#hostname switchB         ！将交换机命名为switchB
switchB(Config)#interface vlan 1        ！进入VLAN1的接口
switchB(Config-if-Vlan1)#ip address 10.1.157.101  255.25.255.0
                                        ！配置VLAN1的IP地址
switchB(Config-if-Vlan1)#no shutdown    ！开启该端口
switchB(Config-if-Vlan1)#exit
switchB(config)#
```

步骤 6：PC1 ping PC2　–t，观察现象。

（1）ping 不通。

（2）所有连接网线的端口的绿灯很频繁地闪烁，表明该端口收发数据量很大，已经在交换机内部形成广播风暴。

（3）当交换机默认开启生成树协议时，不会出现上述现象。

步骤 7：在交换机 A 上启用生成树协议。

```
switchA(config)#spanning-tree               ！启用生成树协议
MSTP is starting now,please wait.............
MSTP is enabled successfully.
switchA(config)#
```

步骤 8：在交换机 B 上启用生成树协议。

```
switchB(config)#spanning-tree               ！启用生成树协议
MSTP is starting now, please wait.............
MSTP is enabled successfully.
switchB(config)#
```

步骤 9：在交换机 A 上验证配置。

```
switchA(config)#show spanning-tree          ！显示生成树协议信息
--MSTP Bridge Config Info--
Standard    :IEEE 802.1s
Bridge MAC  :00:03:0f:13:3f:39
Bridge Times :Max Age 20,Hello Time 2,Forward Delay 15
```

```
Force Version:3
############################ Instance 0 ############################
Self Bridge Id   : 32768-00:03:0f:13:3f:39
Root Id         : this switch
Ext.RootPathCost :0
Region Root Id   :this switch
Int.RootPathCost :0
Root Port ID     :0
Current port list in Instance 0:
Ethernet0/0/1 Ethernet0/0/2(Total 2)
PortName   ID   ExtRPC  IntRPC  State Role    DsgBridge     DsgPort
-------------- ------- --------- --------- --- ---- ---------------- -------
Ethernet0/0/1 128.001   0       0 FWD DSGN 32768.00030f133f39 128.001
Ethernet0/0/2 128.002   0       0 FWD DSGN 32768.00030f133f39 128.002
```

步骤 10：在交换机 B 上验证配置。

```
switchB(config)#show spanning-tree        ！显示生成树协议信息
--MSTP Bridge Config Info--
Standard    :IEEE 802.1s
Bridge MAC  :00:03:0f:13:3f:3d
Bridge Times:  Max Age 20, Hello Time 2,Forward Delay 15
Force Version:3
############################ Instance 0 ############################
Self Bridge Id  : 32768 -  00:03:0f:13:3f:3d
Root Id        : 32768.00:03:0f:13:3f:39
Ext.RootPathCost : 200000
Region Root Id  : this switch
Int.RootPathCost : 0
Root Port ID    : 128.3
Current port list in Instance 0:
Ethernet0/0/3 Ethernet0/0/4 (Total 2)
PortName   ID   ExtRPC  IntRPC  State Role    DsgBridge     DsgPort
-------------- ------- --------- --------- --- ---- ---------------- -------
Ethernet0/0/3 128.003        0 0 FWD ROOT 32768.00030f133f39 128.001
Ethernet0/0/4 128.004         0 0 BLK ALTR 32768.00030f133f39 128.002
switchB(config)#
```

小贴士

交换机 A 和交换机 B 之间的两条链路形成了环路，在两台交换机上配置生成树协议后，交换机 B 的端口 e0/0/4 成为了阻塞端口，所以避免了两台交换机之间由于环路而引起的端口频繁闪烁的不正常现象，此时端口 e0/0/4 是备用端口，连接它的链路成为备用链路，因此也起到了冗余作用。

步骤 11：继续使用 PC1 ping PC2 –t 观察现象。

（1）拔掉交换机 B 端口 4 的网线，观察现象，出现了短暂中断，如图 2-3-3 所示。

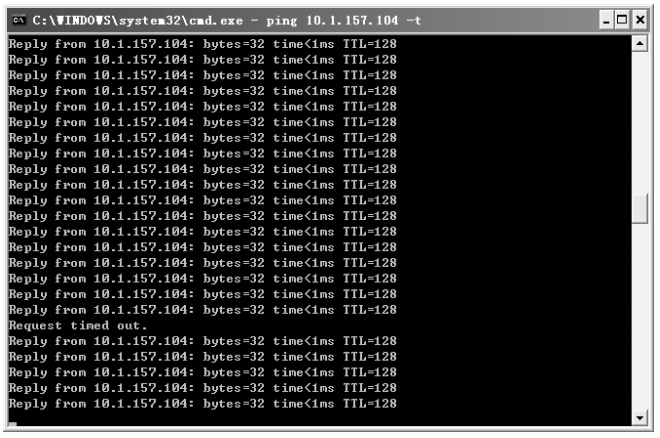


图 2-3-3　PC1 ping PC2 –t 现象（一）

（2）插上交换机 B 端口 4 的网线，观察现象，同样出现了短暂中断，如图 2-3-4 所示。

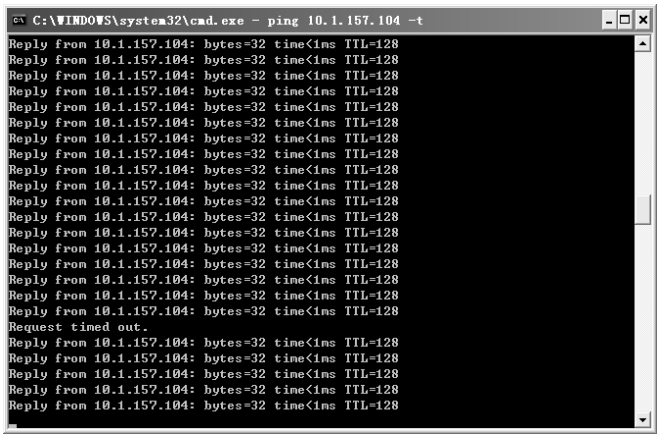


图 2-3-4　PC1 ping PC2 –t 现象（二）

知识拓展

实现多实例生成树技术：由于公司人员增多，部门也随之增多，现公司扩大到 4 台交换机设备，管理员决定采用基于 VLAN 的多实例生成树协议，销售部的 PC1 和 PC3 在 VLAN10 中，技术部的 PC2 和 PC4 在 VLAN 20 中。

所需设备：

（1）DCS-3950 交换机 2 台。

（2）DCRS-5650 交换机 2 台。

（3）PC 4 台。

（4）Console 线 1 条。

（5）双绞线 10 条

实验拓扑结构如图 2-3-5 所示。

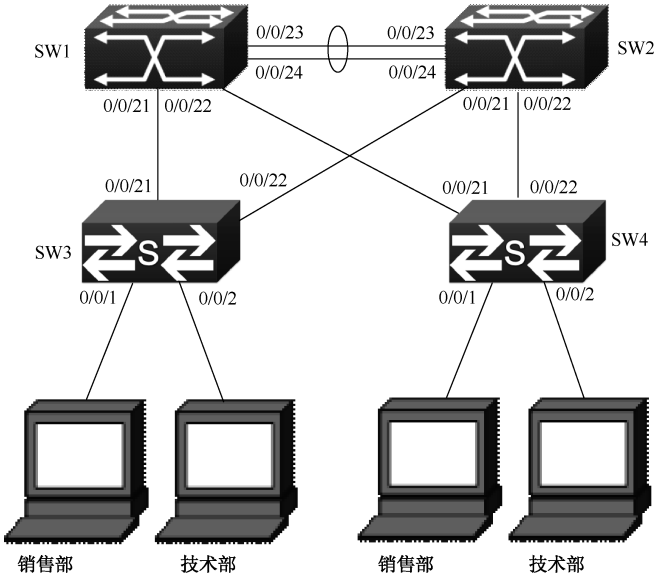


图 2-3-5　实验拓扑结构图

步骤实现

1. 实现端口聚合

由于 SW1 和 SW2 之间的很多数据流量是跨过交换机进行转发的，因此需要增加交换机之间的传输带宽，并实现链路冗余备份，管理员利用聚合端口可实现此功能。

步骤 1：按照图 2-3-5 正确连接拓扑结构图。

步骤 2：交换机恢复出厂设置。

```
switch>enable                                    ! 进入特权配置模式
switch#set default                               ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                    ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 3：配置各个交换机的主机名。

```
Switch(config)#hostname SW1
SW1(config)#
Switch(config)#hostname SW2
SW2(config)#
Switch(config)#hostname SW3
SW3(config)#
Switch(config)#hostname SW4
SW4(config)#
```

步骤 4：在交换机 SW1 上配置聚合端口。

```
SW1(config)#interface e0/0/23-24
SW1(config-If-Port-Range)#switchport mode trunk
SW1(config-If-Port-Range)#port-group 1 mode on
```

步骤 5：在交换机 SW2 上配置聚合端口。

```
SW2(config)#interface e0/0/23-24
SW2(config-If-Port-Range)#switchport mode trunk
SW2(config-If-Port-Range)#port-group 1 mode on
```

2. 实现 MSTP

步骤 1：在 SW1 上启用生成树协议。

```
SW1(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
```

步骤 2：在 SW1 上创建 VLAN 10、VLAN 20，并启动相应端口 Trunk。

```
SW1(config)#vlan 10
SW1(config)#vlan 20
SW1(config)#interface e0/0/21
SW1(config-if-ethernet0/0/21)#switchport mode trunk
SW1(config)#interface e0/0/22
SW1(config-if-ethernet0/0/22)#switchport mode trunk
```

步骤 3：在 SW2 上启用生成树协议。

```
SW2(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
```

步骤 4：在 SW2 上创建 VLAN 10、VLAN 20，并启动相应端口 Trunk。

```
SW2(config)#vlan 10
SW2(config)#vlan 20
SW2(config)#interface e0/0/21
SW2(config-if-ethernet0/0/21)#switchport mode trunk
SW2(config)#interface e0/0/22
SW2(config-if-ethernet0/0/22)#switchport mode trunk
```

步骤 5：在 SW3 上启用生成树协议。

```
SW3(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
```

步骤 6：在 SW3 上创建 VLAN 10、VLAN 20，把相应端口分配给 VLAN 并启动相应端口 Trunk。

```
SW3(config)#vlan 10
SW3(config)#vlan 20
SW3(config)#interface e0/0/1
SW3(config-if- ethernet0/0/1)#switchport access vlan 10
SW3(config)#interface e0/0/2
SW3(config-if- ethernet0/0/2)#switchport access vlan 20
SW3(config)#interface e0/0/21
SW3(config-if- ethernet0/0/21)#switchport mode trunk
SW3(config)#interface e0/0/22
SW3(config-if- ethernet0/0/22)#switchport mode trunk
```

步骤 7：在 SW4 上启用生成树协议。

```
SW4(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
```

步骤 8：在 SW4 上创建 VLAN 10、VLAN 20，把相应端口分配给 VLAN 并启动相应端口 Trunk。

```
SW4(config)#vlan 10
SW4(config)#vlan 20
SW4(config)#interface e0/0/1
SW4(config-if- ethernet0/0/1)#switchport access vlan 10
SW4(config)#interface e0/0/2
SW4(config-if- ethernet0/0/2)#switchport access vlan 20
SW4(config)#interface e0/0/21
SW4(config-if- ethernet0/0/21)#switchport mode trunk
SW4(config)#interface e0/0/22
SW4(config-if- ethernet0/0/22)#switchport mode trunk
```

步骤 9：在 SW1 上配置实例 1 关联 VLAN 10、实例 2 关联 VLAN 20，并配置名称和版本。

```
SW1(config)#spanning-tree mst configuration
SW1(config-mstp-region)#revision-level 1
SW1(config-mstp-region)#name region1
SW1(config-mstp-region)#instance 1 vlan 10
SW1(config-mstp-region)#instance 2 vlan 20
SW1(config-mstp-region)#
```

步骤 10：在 SW2 上配置实例 1 关联 VLAN 10、实例 2 关联 VLAN 20，并配置名称和版本。

```
SW2(config)#spanning-tree mst configuration
SW2(config-mstp-region)#revision-level 1
SW2(config-mstp-region)#name region1
SW2(config-mstp-region)#instance 1 vlan 10
SW2(config-mstp-region)#instance 2 vlan 20
SW2(config-mstp-region)#
```

步骤 11：在 SW3 上配置实例 1 关联 VLAN 10、实例 2 关联 VLAN 20，并配置名称和版本。

```
SW3(config)#spanning-tree mst configuration
SW3(config-mstp-region)#revision-level 1
SW3(config-mstp-region)#name region1
SW3(config-mstp-region)#instance 1 vlan 10
SW3(config-mstp-region)#instance 2 vlan 20
SW3(config-mstp-region)#
```

步骤 12：在 SW4 上配置实例 1 关联 VLAN 10、实例 2 关联 VLAN 20，并配置名称和版本。

```
SW4(config)#spanning-tree mst configuration
SW4(config-mstp-region)#revision-level 1
SW4(config-mstp-region)#name region1
SW4(config-mstp-region)#instance 1 vlan 10
SW4(config-mstp-region)#instance 2 vlan 20
```

```
SW4(config-mstp-region)#
```

步骤 13： 在 SW1 和 SW2 上配置优先级。

```
SW1(config)# spanning-tree mst 1 priority 0
//配置优先级，使其成为instance（实例） 1中的根
SW1(config)# spanning-tree mst 2 priority 4096
SW2(config)#spanning-tree mst 1 priority 4096
SW2(config)#spanning-tree mst 2 priority 0
//配置优先级，使其成为instance（实例）2中的根
```

步骤 14：验证交换机 SW3 的生成树协议的配置。

```
SW3#show spanning-tree mst config
Name        region1
Revision     1
Instance     Vlans Mapped
----------------------------------
00          1-9, 11-19, 21-4094
01          10
02          20
----------------------------------
```

步骤 15：测试每个 VLAN 是否都是无环的链路。

```
SW4#show spanning-tree interface e0/0/22
Ethernet0/0/22:
Mst   ID      IntRPC   State Role    DsgBridge      DsgPort VlanCount
--- ------- ---------   --- ---- ------------------ ------- ---------
  0 128.022         0   FWD  DSGN 32768.00030f1324dd 128.022         1
  1 128.022    100000   BLK  ALTR  4096.00030f1da543 128.022        1
  2 128.022         0   FWD  ROOT     0.00030f1da543 128.022         1
```

学习小结

本学习活动介绍了交换机生成树协议，它可以在互联网中提供多条冗余备份链路，并解决互联网中的环路问题。默认情况下，两个交换机间的多条冗余链路仅有一条处于工作状态，其他链路处于关闭状态，只有当其他链路出现故障或断开的情况下才会启用。但如果设置了生成树的 VLAN 负载均衡技术，就可以实现多条链路的同时工作，这在一定程度上实现了网络带宽的拓容，从而提升了网络的速度。

学习活动 3　交换机的 DHCP 服务

动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是 TCP/IP 协议族中的一种，主要作用是给网络中其他计算机动态分配 IP 地址。

学习情境

某公司总经理发现自己的计算机“ IP 地址冲突”，并且上不了网，于是找来网络管理员解决该问题，管理员认为是有员工擅自修改 IP 地址导致的，可以通过在现有的三层交换机上使用 DHCP 技术来解决该问题。

情境分析

网络管理员为每一台计算机手动分配一个 IP 地址，这样将会大大加重网络管理员的负担，还容易导致 IP 地址分配错误，有什么办法既能减少管理员的工作量、降低输入错误的可能，还能避免 IP 地址冲突呢？网络管理员的想法非常正确，而且不需要再增加硬件就可以实现。

所需设备：

（1）DCR-5650 交换机 1 台。

（2）PC 1 台。

（3）直连线 1 条。

学习活动拓扑结构如图 2-3-6 所示。

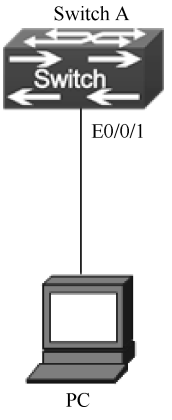


图 2-3-6　交换机的 DHCP

相关知识

DHCP 是由服务器控制的一段 IP 地址范围，客户机登录服务器时可以自动获得服务器分配的 IP 地址、子网掩码、网关和 DNS 地址。首先，网络中必须存在一台 DHCP 服务器，这台服务器可以是采用 Windows Server 2003 系统的计算机，也可以是交换机或路由器；其次，客户机要设置为自动获取 IP 地址的方式才能正常获取 DHCP 服务器提供的 IP 地址。本学习活动使用三层交换机作为 DHCP 服务器实现动态分配 IP 地址。

步骤实现

步骤 1：按照图 2-3-6 正确连接拓扑结构。

步骤 2：将交换机恢复出厂设置。

```
switch#set default                          ! 恢复出厂设置
switch#write                                ! 保存配置
switch#reload                               ! 重启交换机
```

步骤 3：为交换机设置名称并配置接口 IP 地址。

```
DCRS-5650-28>enable                                          ! 进入特权模式
DCRS-5650-28#config                                          ! 进入全局配置模式
DCRS-5650-28(config)#hostname SwitchA                        ! 修改机器名称
SwitchA(config)#interface vlan 1                             ! 进入VLAN模式
SwitchA(Config-if-Vlan1)#ip address 192.168.2.1 255.255.255.0
                                                             ! 配置IP地址
```

```
SwitchA(Config-if-Vlan1)#no shutdown
SwitchA(Config-if-Vlan1)#^Z                    ！按【Ctrl+Z】组合键进入特权模式
```

步骤 4：DHCP 服务器的配置。

```
SwitchA#config
SwitchA(config)#service dhcp                                    ！启动DHCP服务
SwitchA(config)#ip dhcpd pool testA                             ！定义地址池
SwitchA(dhcp-testA-config)#network 192.168.2.0 24               ！定义网络号
SwitchA(dhcp-testA-config)#lease 1                              ！定义租约为1天
SwitchA(dhcp-testA-config)#default-router 192.168.2.1           ！定义默认网关
SwitchA(dhcp-testA-config)#dns-server  202.96.128.86            ！定义DNS服务器
SwitchA(dhcp-testA-config)#exit
SwitchA(config)#ip dhcp excluded-address 192.168.2.2 192.168.2.9
```

步骤 5：配置 PC 及验证获得的地址。

（1）设置 PC 的 IP 地址，如图 2-3-7 所示。

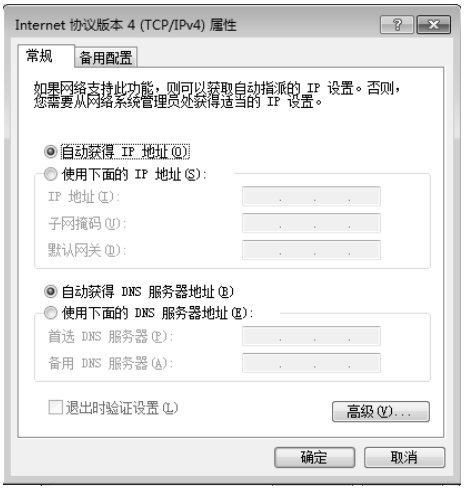


图 2-3-7　配置 PC 的 IP 地址

（2）执行“开始”→“运行”命令，在文本框内输入“cmd”，在命令行窗口中输入“ipconfig/all”，如图 2-3-8 所示。

C:\Windows\system32\cmd.exe
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Realtek PCIe GBE Family Controller
物理地址. . . . . : A4-1F-72-85-97-54
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::39f3:dd32:d509:3665x13(首选)
IPv4 地址 . . . . . : 192.168.1.11(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2014年5月4日 15:47:50
租约过期的时间 . . . . . : 2014年5月5日 15:47:50
默认网关. . . . . : 192.168.1.1
DHCP 服务器 . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 195305330
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-1A-06-44-8C-A4-1F-72-85-97-54
DNS 服务器 . . . . . : 202.96.128.86
TCPIP 上的 NetBIOS . . . . . : 已启用
以太网适配器 VirtualBox Host-Only Network:

图 2-3-8　DHCP 验证效果图

知识拓展

路由器 DHCP 服务的配置所需设备如下：

（1）DCR-2655 路由器 1 台。

（2）PC 1 台。

（3）交叉线 1 条。

实验拓扑结构如图 2-3-9 所示。

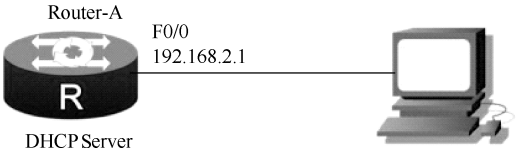


图 2-3-9　DHCP 配置拓扑结构

步骤 1：按照图 2-3-9 正确连接拓扑结构。

步骤 2：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 3：为路由器设置主机名称和配置接口 IP 地址。

```
Router>enable                                      ！进入特权模式
Router #config                                     ！进入全局配置模式
Router _config#hostname Router-A                   ！修改机器名称
Router-A_config#interface f0/0                     ！进入接口模式
Router-A_config_ f0/0#ip address 192.168.2.1 255.255.255.0  ！配置IP地址
Router-A config  f0/0#no shutdown
Router-A_config_ f0/0#^Z                       ！按【Ctrl+Z】组合键进入特权模式
```

步骤 4：DHCP 服务器的配置。

```
Router-A#conf
Router-A _config#ip dhcpd pool 1                              ！定义地址池
Router-A _config_dhcp#network 192.168.2.0 255.255.255.0       ！定义网络号
Router-A _config_dhcp#range 192.168.2.10 192.168.2.20         ！定义地址范围
Router-A _config_dhcp#lease 1                                 ！定义租约为1天
Router- A_config_dhcp#exit
Router-A_config#ip dhcpd enable                               ！启动DHCP服务
```

步骤 5：验证。

```
Router-A#sh ip dhcp pool
DHCP Server Address Pool Information:
Pool 1 :
```

```
Network : 192.168.2.0
Range : 192.168.2.10 - 192.168.2.20
Total address : 11
Leased address : 1
Abandoned address : 0
Available address : 10
```

步骤 6：配置 PC 及验证获得的地址。

（1）设置 PC 的 IP 地址，如图 2-3-10 所示。

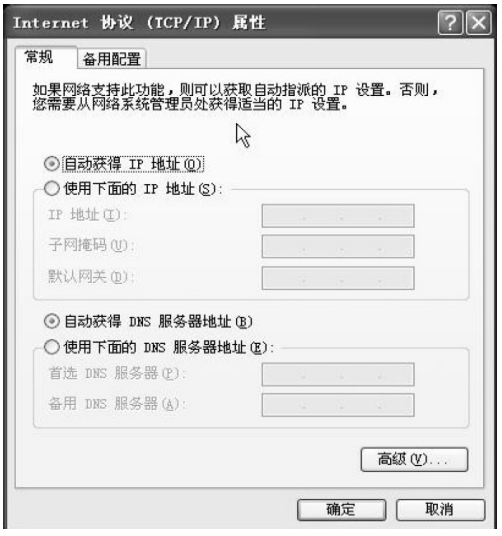


图 2-3-10　设置 PC 的 IP 地址

（2）执行“开始”→“运行”命令，在“打开”文本框内输入“cmd”，在命令行窗口中输入“ipconfig/all”，如图 2-3-11 所示。

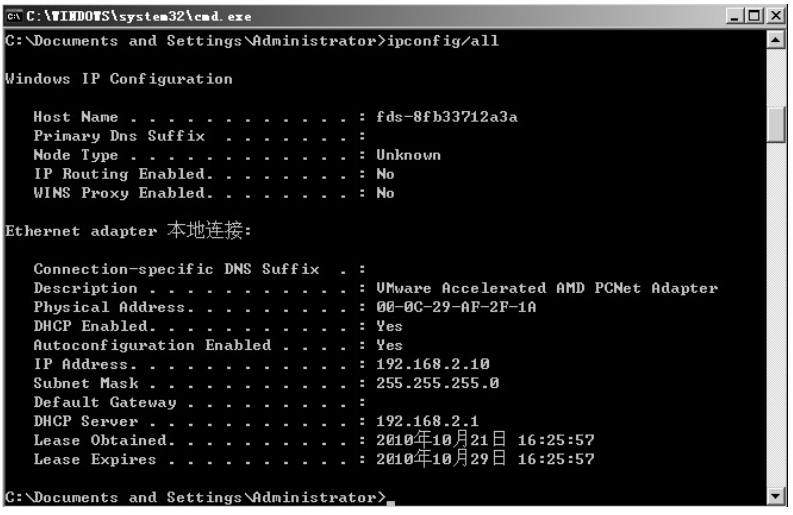

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig/all
Windows IP Configuration
Host Name . . . . . : fds-8fb33712a3a
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 00-0C-29-AF-2F-1A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.2.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.2.1
Lease Obtained. . . . . : 2010年10月21日 16:25:57
Lease Expires . . . . . : 2010年10月29日 16:25:57
C:\Documents and Settings\Administrator>

图 2-3-11　DHCP 验证效果图

学习小结

本学习活动介绍了交换机的 DHCP 服务，可以使下连的计算机通过交换机获取 IP 地址、子网掩码、网关和 DNS 服务器地址。当一个网络中计算机数量庞大时，使用 DHCP 服务，可以很方便地为每一台计算机配置好相应的 IP 参数，减轻了网络管理员分配 IP 的工作负担。

学习活动 4　交换机的 VRRP 服务

虚拟路由器冗余协议（Virtual Router Redundancy Protocol，VRRP）是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。使用 VRRP 的好处是有更高默认的路径的可用性而无须在每个终端主机上配置动态路由或路由发现协议。

学习情境

公司企业网络核心层原来使用一台三层交换机，随着网络应用的日益增多，对网络的可靠性也提出了越来越高的要求，公司决定采用默认网关进行冗余备份，以便在其中一台设备出现故障时，备份设备能够及时接管数据转发工作，为用户提供透明的切换，提高网络的稳定性。

情境分析

可用两台三层交换机作为核心层设备，采用 VRRP 技术使两台交换机互相备份，以此来提高网络的可靠性和稳定性。

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）DCS-3950 交换机 1 台。

（3）Console 线 1 条。

（4）PC 3 台。

（5）交叉线 3 条。

（6）直连线 3 条。

交换机的 VRRP 服务拓扑结构如图 2-3-12 所示。

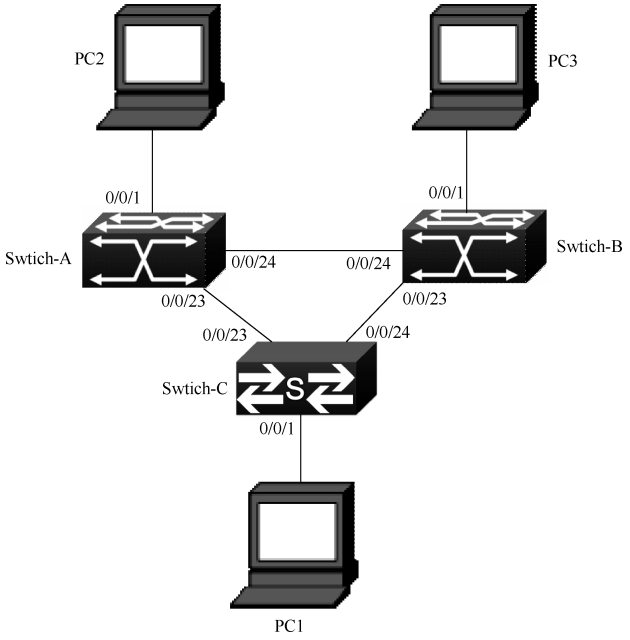


图 2-3-12　交换机的 VRRP 服务拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 2-3-4。

表 2-3-4　交换机和 PC 的 IP 地址网络参数设置

设　　备	端　　口	IP 地址	子网掩码	网　　关
Switch-A 的 VLAN10	E0/0/1	192.168.10.1	255.255.255.0	无
Switch-A 的 VLAN100	E0/0/24	192.168.100.1	255.255.255.0	无
Switch-B 的 VLAN20	E0/0/1	192.168.20.1	255.255.255.0	无
Switch-B 的 VLAN100	E0/0/24	192.168.100.2	255.255.255.0	无
Switch-C 的 VLAN100	E0/0/1	无	无	无
PC1		192.168.100.100	255.255.255.0	192.168.100.254
PC2		192.168.10.2	255.255.255.0	192.168.10.1
PC3		192.168.20.2	255.255.255.0	192.168.20.1

相关知识

VRRP 是由 IETF 提出的用于解决局域网中配置静态网关出现单点失效现象的路由协议，1998 年已推出正式的 RFC 2338 协议标准。VRRP 广泛应用在边缘网络中，它的设计目标是支持特定情况下 IP 数据流量失败转移不会引起混乱，允许主机使用单路由器，以及及时在实际第一跳路由器使用失败的情形下仍能够维护路由器间的连通性。

VRRP 是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台上。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。VRRP 是一种 LAN

接入设备备份协议。一个局域网络内的所有主机都设置了默认网关，这样主机发出的目的地址不在本网段的报文将被通过默认网关发往三层交换机，从而实现了主机和外部网络的通信。

VRRP 是一种路由容错协议，也可以叫做备份路由协议。一个局域网络内的所有主机都设置默认路由，当网内主机发出的目的地址不在本网段时，报文将被通过默认路由发往外部路由器，从而实现了主机与外部网络的通信。当默认路由器 down（即端口关闭）之后，内部主机将无法与外部通信，如果路由器设置了 VRRP，那么虚拟路由将启用备份路由器，从而实现全网通信。

参考命令配置如下：

```
Switch#config
Switch(config)#router vrrp 1                              !启动VRRP组
Switch(config-router)#virtual-ip 192.168.100.254          !虚拟IP地址
Switch(config-router)#int vlan 100
Switch(config-router)#priority 150                        !优先级
Switch(config-router)#enable                              !在VLAN100中生效
Switch(config-router)#
```

步骤实现

步骤 1：按照图 2-3-12 正确连接拓扑结构。

步骤 2：按照表 2-3-4 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：将交换机恢复出厂设置。

```
switch>enable                                             !进入特权配置模式
switch#set default                                        !恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                             !重启交换机
Process with reboot? [Y/N]y
```

步骤 4：配置交换机 A 的主机名称和划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname Switch-A
Switch-A(config)#vlan 10
Switch-A(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
Switch-A(Config-Vlan10)#exit
Switch-A(config)#vlan 100
Switch-A(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
Switch-A(Config-Vlan100)#exit
Switch-A(config)#
```

步骤 5：配置交换机 B 的主机名称和划分 VLAN。

```
DCRS-5650-28>
```

```
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  Switch-B
Switch-B(config)#vlan 20
Switch-B(Config-Vlan20)#exit
Switch-B(Config-Vlan20)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
Switch-B(config)#vlan 100
Switch-B(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
Switch-B(Config-Vlan100)#exit
Switch-B(config)#
```

步骤 6：配置交换机 C 的主机名称和划分 VLAN。

```
DCS-3950-26C#enable
DCS-3950-26C#config
DCS-3950-26C(config)#hostname Switch-C
Switch-C(config)#vlan 100
Switch-C(config-vlan100)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 100 successfully
Switch-C(config-vlan100)#
```

步骤 7：配置交换机 A 的 23 端口为 Trunk。

```
Switch-A#
Switch-A#config
Switch-A(config)#int e0/0/23
Switch-A(Config-If-Ethernet0/0/23)#switchport mode trunk
Set the port Ethernet0/0/23 mode TRUNK successfully
Switch-A(Config-If-Ethernet0/0/23)#
```

步骤 8：配置交换机 B 的 23 端口为 Trunk。

```
Switch-B#
Switch-B#config
Switch-B(config)#int e0/0/23
Switch-B(Config-If-Ethernet0/0/23)#switchport mode trunk
Set the port Ethernet0/0/23 mode TRUNK successfully
Switch-B(Config-If-Ethernet0/0/23)#
```

步骤 9：配置交换机 C 的 23 和 24 端口为 Trunk。

```
Switch-C(config)#int e0/0/23
Switch-C(config-if-ethernet0/0/23)#switchport mode trunk
Set the port Ethernet0/0/23 mode TRUNK successfully
Switch-C(config-if-ethernet0/0/23)#int e0/0/24
Switch-C(config-if-ethernet0/0/24)#switchport mode trunk
Set the port Ethernet0/0/24 mode TRUNK successfully
Switch-C(config-if-ethernet0/0/24)#
Switch-C#config
```

步骤 10：查看交换机 A 上划分的 VLAN。

```
Switch-A#show vlan
VLAN Name        Type      Media    Ports
---- ----------- --------- -------- ------------------------------------
1    default     Static    ENET     Ethernet0/0/2      Ethernet0/0/3
                                    Ethernet0/0/4      Ethernet0/0/5
                                    Ethernet0/0/6      Ethernet0/0/7
                                    Ethernet0/0/8      Ethernet0/0/9
                                    Ethernet0/0/10     Ethernet0/0/11
                                    Ethernet0/0/12     Ethernet0/0/13
                                    Ethernet0/0/14     Ethernet0/0/15
                                    Ethernet0/0/16     Ethernet0/0/17
                                    Ethernet0/0/18     Ethernet0/0/19
                                    Ethernet0/0/20     Ethernet0/0/21
                                    Ethernet0/0/22     Ethernet0/0/23(T)
                                    Ethernet0/0/25     Ethernet0/0/26
                                    Ethernet0/0/27     Ethernet0/0/28
20   VLAN0010    Static    ENET     Ethernet0/0/1      Ethernet0/0/23(T)
100  VLAN0100    Static    ENET     Ethernet0/0/23(T)  Ethernet0/0/24
Switch-A#
```

步骤 11：查看交换机 B 上划分的 VLAN。

```
Switch-B#show vlan
VLAN Name        Type      Media    Ports
---- ----------- --------- -------- ------------------------------------
1    default     Static    ENET     Ethernet0/0/2      Ethernet0/0/3
                                    Ethernet0/0/4      Ethernet0/0/5
                                    Ethernet0/0/6      Ethernet0/0/7
                                    Ethernet0/0/8      Ethernet0/0/9
                                    Ethernet0/0/10     Ethernet0/0/11
                                    Ethernet0/0/12     Ethernet0/0/13
                                    Ethernet0/0/14     Ethernet0/0/15
                                    Ethernet0/0/16     Ethernet0/0/17
                                    Ethernet0/0/18     Ethernet0/0/19
                                    Ethernet0/0/20     Ethernet0/0/21
                                    Ethernet0/0/22     Ethernet0/0/23(T)
                                    Ethernet0/0/25     Ethernet0/0/26
                                    Ethernet0/0/27     Ethernet0/0/28
20   VLAN0020    Static    ENET     Ethernet0/0/1      Ethernet0/0/23(T)
100  VLAN0100    Static    ENET     Ethernet0/0/23(T)   Ethernet0/0/24
Switch-B#
```

步骤 12：查看交换机 C 上划分的 VLAN。

```
Switch-C##show vlan
VLAN Name        Type      Media    Ports
---- ----------- --------- --------- ------------------------------------
1    default     Static    ENET        Ethernet0/0/2     Ethernet0/0/3
```

```
                                        Ethernet0/0/4      Ethernet0/0/5
                                        Ethernet0/0/6      Ethernet0/0/7
                                        Ethernet0/0/8      Ethernet0/0/9
                                        Ethernet0/0/10     Ethernet0/0/11
                                        Ethernet0/0/12     Ethernet0/0/13
                                        Ethernet0/0/14     Ethernet0/0/15
                                        Ethernet0/0/16     Ethernet0/0/17
                                        Ethernet0/0/18     Ethernet0/0/19
                                        Ethernet0/0/20     Ethernet0/0/21
                                        Ethernet0/0/22     Ethernet0/0/23(T)
                                        Ethernet0/0/24(T)  Ethernet0/0/25
                                        Ethernet0/0/26
100  VLAN0100     Static     ENET       Ethernet0/0/1      Ethernet0/0/23(T)
                                        Ethernet0/0/24(T)

Switch-C#
```

步骤 13：在交换机 A 的接口上配置 IP 地址。

```
Switch-A(config)#int vlan 10
Switch-A(Config-if-Vlan10)#ip add 192.168.10.1 255.255.255.0
Switch-A(Config-if-Vlan10)#no shut
Switch-A(Config-Vlan10)#exit
Switch-A(config)#int vlan 100
Switch-A(Config-if-Vlan100)#ip add 192.168.100.1 255.255.255.0
Switch-A(Config-if-Vlan100)#no shut
Switch-A(Config-Vlan100)#exit
```

步骤 14：查看交换机 A 接口上的配置情况。

```
Switch-A#show ip int brief
Index    Interface            IP-Address    Status             Protocol
2002     Loopback             127.0.0.1       up                   up
2004     Vlan10               192.168.10.1    up                   up
2005     Vlan100              192.168.100.1   up                   up


Switch-A#
```

步骤 15：在交换机 B 的接口上配置 IP 地址。

```
Switch-B(config)#int vlan 20
Switch-B(Config-if-Vlan20)#ip add 192.168.20.1 255.255.255.0
Switch-B(Config-if-Vlan20)#no shut
Switch-B(Config-Vlan20)#exit
Switch-B(config)#int vlan 100
Switch-B(Config-if-Vlan100)#ip add 192.168.100.2 255.255.255.0
Switch-B(Config-if-Vlan100)#no shut
Switch-B(Config-Vlan40)#exit
```

步骤 16：查看交换机 B 的接口上的配置情况。

```
Switch-B#show ip int brief
Index    Interface            IP-Address    Status             Protocol
```

```
2002     Loopback            127.0.0.1       up                  up
2004     Vlan20              192.168.20.1    up                  up
2005     Vlan100             192.168.100.2   up                  up

Switch-B#
```

步骤 17：开启交换机 A 的生成树协议，防止环路出现。

```
Switch-A(config)#
Switch-A(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
Switch-A(config)#
```

步骤 18：开启交换机 B 的生成树协议，防止环路出现。

```
Switch-B(config)#
Switch-B(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
Switch-B(config)#
```

步骤 19：开启交换机 C 的生成树协议，防止环路出现。

```
Switch-C(config)#
Switch-C(config)#spanning-tree
MSTP is starting now, please wait.....
MSTP is enabled successfully.
Switch-C(config)#
```

步骤 20：配置交换机 A 到 PC3 的静态路由。

```
Switch-A(config)#
Switch-A(config)#ip route 192.168.20.0 255.255.255.0 192.168.100.2
Switch-A(config)#
```

步骤 21：配置交换机 B 到 PC2 的静态路由。

```
Switch-B(config)#
Switch-B(config)#ip route 192.168.10.0 255.255.255.0 192.168.100.1
Switch-B(config)#
```

步骤 22：查看交换机 A 的路由表。

```
Switch-A#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.10.0/24 is directly connected, Vlan10
S       192.168.20.0/24 [1/0] via 192.168.100.2, Vlan100
C       192.168.100.0/24 is directly connected, Vlan100
```

```
Total routes are : 4 item(s)
Switch-A#
```

步骤 23：查看交换机 B 的路由表。

```
Switch-B#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
S       192.168.10.0/24 [1/0] via 192.168.100.1, Vlan100
C       192.168.20.0/24 is directly connected, Vlan20
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
Switch-B#
```

步骤 24：测试网络的连通性，此时全网已经互通，如图 2-3-13 所示。

步骤 25：在交换机 A 上配置 VRRP。

```
Switch-A#config
Switch-A(config)#router vrrp 1
Switch-A(config-router)#virtual-ip 192.168.100.254  ！虚拟网关IP地址
Switch-A(config-router)#int vlan 100
Switch-A(config-router)#enable
Switch-A(config-router)#
```

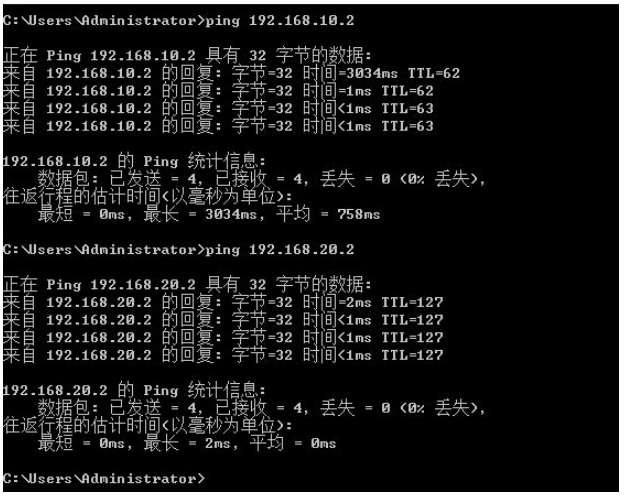


图 2-3-13　连通性测试效果图（一）

步骤 26：在交换机 B 上配置 VRRP。

```
Switch-B#config
Switch-B(config)#router vrrp 1
Switch-B(config-router)#virtual-ip 192.168.100.254
```

```
Switch-B(config-router)#int vlan 100
Switch-B(config-router)#priority 150  ！优先级
Switch-B(config-router)#enable
Switch-B(config-router)#
```

步骤 27：查看交换机 A 上的 VRRP 配置。

```
Switch-A#show vrrp
VrId 1
 State is Backup              ！此交换机为备份
 Virtual IP is 192.168.100.254 (Not IP owner)
 Interface is Vlan100
 Priority is 100              ！默认优先级，所以此交换机为备份
 Advertisement interval is 1 sec
 Preempt mode is TRUE
Switch-A#
```

步骤 28：查看交换机 B 上的 VRRP 配置。

```
Switch-B#show vrrp
VrId 1
 State is Master              ！此交换机为主
 Virtual IP is 192.168.100.254 (Not IP owner)
 Interface is Vlan100
 Priority is 150              ！优先级为150，所以此交换机为主
 Advertisement interval is 1 sec
 Preempt mode is TRUE
Switch-B#
```

步骤 29：测试网络的连通性。

（1）在 PC1 上 ping PC2 的 IP 地址 192.168.10.2，网络是连通的，将交换机 B 和交换机 C 之间的网线拔掉，断了几秒后，仍然是连通的，如图 2-3-14 所示。

（2）在 PC1 上 ping PC3 的 IP 地址 192.168.20.2，网络是连连通的，将交换机 B 和交换机 C 之间的网线拔掉，断了几秒后，仍然是连通的，如图 2-3-15 所示。

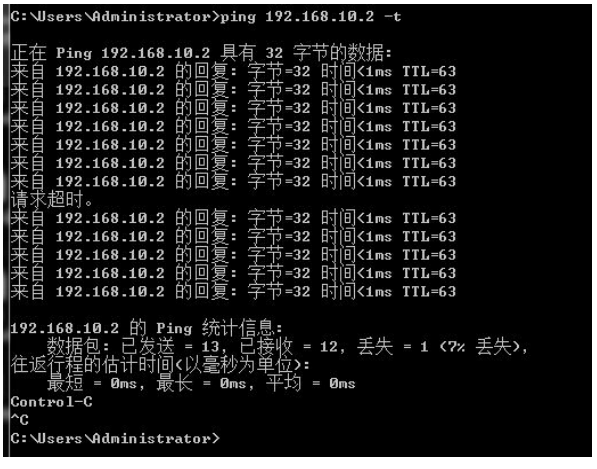


图 2-3-14　连通性测试效果图（二）

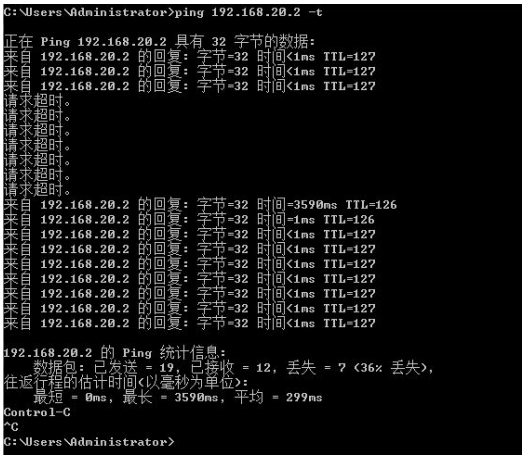


图 2-3-15　连通性测试效果图（三）

学习小结

本学习活动学习了 VRRP 服务，VRRP 将网络中的两台三层交换机组成 VRRP 冗余组，针对于网络中每一个 VLAN 接口，都拥有一个虚拟默认网关地址。各个 VLAN 内的主机通过这个虚拟 IP 访问外网资源。如果活动交换机发生了故障，VRRP 将自动使用备份交换机来替代活动交换机。由于网络内的终端配置了 VRRP 虚拟网关地址，当发生故障时，虚拟交换机没有改变，主机仍然保持连接，网络将不会受到单点故障的影响，这样就很好地解决了网络中核心交换机切换的问题。

学习任务 4　交换机的路由配置

交换机划分 VLAN 后可以连接多个不同的网络。当然，网络中存在多个交换机互连时，要实现交换机间多个不同网络的通信时，要在交换机上配置路由协议。交换机提供的路由协议包括静态路由协议、RIP 动态路由协议和 OSPF 动态路由协议等。本学习任务针对以上三种路由协议进行配置。

学习活动 1　交换机间的静态路由配置。

学习活动 2　交换机间的 RIP 动态路由配置。

学习活动 3　交换机间的 OSPF 动态路由配置。

学习活动 1　交换机间的静态路由配置

静态路由是指由网络管理员手工配置的路由信息。当网络的拓扑结构或链路状态发生变化时，网络管理员要手工修改路由表中的静态路由信息。静态路由信息在默认情况下不会传递给其他的路由器。静态路由一般适用于比较简单的网络环境。

学习情境

某公司刚成立，规模很小，只有两台基于交换机的小型网络。该公司的网络管理员经过考虑，决定在公司的交换机间使用静态路由，实现网络的互连。

情境分析

由于该网络规模较小且不经常变动，所以使用静态路由比较合适。两台交换机之间通过以太网口相连，每台交换机连接两台计算机。

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）PC 4 台。
（3）交叉线 1 条。
（4）直连线 4 条。
静态路由拓扑图如图 2-4-1 所示。

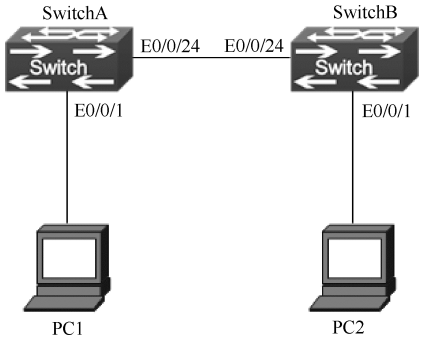


图 2-4-1　静态路由拓扑图

交换机和 PC 的 IP 地址网络参数设置见表 2-4-1。

表 2-4-1　交换机和 PC 的 IP 地址网络参数设置

设　　备	端　　口	IP 地址	子网掩码	网关 1
SwitchA 的 VLAN10	E0/0/1	192.168.10.1	255.255.255.0	无
SwitchA 的 VLAN100	E0/0/24	192.168.100.1	255.255.255.0	无
SwitchB 的 VLAN20	E0/0/1	192.168.20.1	255.255.255.0	无
SwitchB 的 VLAN100	E0/0/24	192.168.100.2	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

相关知识

静态路由（Static Route）是一种特殊的路由，由网络管理员手工配置。在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通，路由效率也非常高。合理设置和使用静态路由可以改善网络的性能，并可以为重要的网络应用保证带宽。

但静态路由也有其自身的缺点：不能自动适应网络拓扑结构的变化，当网络拓扑结构发生变化时，可能会出现路由不可达，导致网络中断情况。此时需要网络管理员手工修改静态路由的配置。另外，网络结构比较复杂时，静态路由表可能会非常庞大，这样反而会影响效率。所以静态路由一般只适用于只有几级路由结点的小型网络中。一般而言，当路由跳数大于 5 时就不建议使用静态路由，而采用后面将要介绍动态路由。

配置静态路由时，需要了解以下内容。

（1）目的地址与掩码。在 ip route 命令中，IPv4 地址为点分十进制格式，掩码也同样用点分十进制格式表示。

（2）出口和下一跳地址。在配置静态时，可通过参数 interface-type interface-number（其实也就是我们习惯使用的 interface-id 参数）指定数据包在路由器上的出口，也可以指定下一

跳地址。指定出口还是下一跳地址要视具体情况而定，但下一跳地址不能为本地接口 IP 地址，否则路由不会生效。实际上，所有的路由项都必须明确下一跳地址。在发送报文时，首先根据报文的目的地址寻找路由表中与之匹配的路由，只有指定了下一跳地址，链路层才能找到对应的链路层地址，并转发报文。

（3）其他属性。对于不同的静态路由，可以为它们配置不同的优先级，从而更灵活地应用路由管理策略，但不是必需的。例如，配置达到相同目的地的多条路由，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份。

静态路由就是手工配置的路由，使得到指定目标网络的数据包传送，按照预定的路径进行。当路由器不能学习到某些目标网络的路由时，配置静态路由就显得十分重要。

在小型的网络中，使用静态路由是较好的选择，管理员想控制数据转发路径时，也会使用静态路由。

静态路由的配置命令如下：

```
ip route 目的网络的IP 地址 子网掩码 下一跳IP地址/本地接口
```

步骤实现

步骤 1：按照图 2-4-1 连接网络拓扑结构。

步骤 2：按照表 2-4-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          !进入特权配置模式
switch#set default                                     !恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          !重启交换机
Process with reboot? [Y/N]y
```

步骤 4：在交换机 A 上配置主机名和划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchA
SwitchA(config)#vlan 10
SwitchA(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
SwitchA(Config-Vlan10)#exit
SwitchA(config)#vlan 100
SwitchA(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchA(Config-Vlan100)#exit
SwitchA(config)#
```

步骤 5：查看交换机 A 上划分的 VLAN。

```
SwitchA#show vlan
VLAN Name        Type      Media     Ports
```

```
---- ----------- --------- -------- ---------------------------------------
1    default      Static    ENET     Ethernet0/0/2      Ethernet0/0/3
                                     Ethernet0/0/4      Ethernet0/0/5
                                     Ethernet0/0/6      Ethernet0/0/7
                                     Ethernet0/0/8      Ethernet0/0/9
                                     Ethernet0/0/10     Ethernet0/0/11
                                     Ethernet0/0/12     Ethernet0/0/13
                                     Ethernet0/0/14     Ethernet0/0/15
                                     Ethernet0/0/16     Ethernet0/0/17
                                     Ethernet0/0/18     Ethernet0/0/19
                                     Ethernet0/0/20     Ethernet0/0/21
                                     Ethernet0/0/22     Ethernet0/0/23
                                     Ethernet0/0/25     Ethernet0/0/26
                                     Ethernet0/0/27     Ethernet0/0/28
10   VLAN0010     Static    ENET     Ethernet0/0/1
100  VLAN0100     Static    ENET     Ethernet0/0/24
SwitchA#
```

步骤 6：在交换机 B 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchB
SwitchB(config)#vlan 20
SwitchB(Config-Vlan20)#exit
SwitchB(Config-Vlan20)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
SwitchB(config)#vlan 100
SwitchB(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchB(Config-Vlan100)#exit
SwitchB(config)#
```

步骤 7：查看交换机 B 上划分的 VLAN。

```
SwitchB#show vlan
VLAN Name        Type      Media     Ports
---- ----------- --------- -------- ---------------------------------------
1    default      Static    ENET     Ethernet0/0/2      Ethernet0/0/3
                                     Ethernet0/0/4      Ethernet0/0/5
                                     Ethernet0/0/6      Ethernet0/0/7
                                     Ethernet0/0/8      Ethernet0/0/9
                                     Ethernet0/0/10     Ethernet0/0/11
                                     Ethernet0/0/12     Ethernet0/0/13
                                     Ethernet0/0/14     Ethernet0/0/15
                                     Ethernet0/0/16     Ethernet0/0/17
                                     Ethernet0/0/18     Ethernet0/0/19
```

```
                                    Ethernet0/0/20      Ethernet0/0/21
                                    Ethernet0/0/22      Ethernet0/0/23
                                    Ethernet0/0/25      Ethernet0/0/26
                                    Ethernet0/0/27      Ethernet0/0/28
20   VLAN0020     Static     ENET    Ethernet0/0/1
100  VLAN0100     Static     ENET    Ethernet0/0/24
SwitchB#
```

步骤 8：在交换机 A 接口上配置 IP 地址。

```
SwitchA(config)#int vlan 10
SwitchA(Config-if-Vlan10)#ip add 192.168.10.1 255.255.255.0
SwitchA(Config-if-Vlan10)#no shut
SwitchA(Config-Vlan10)#exit
SwitchA(config)#int vlan 100
SwitchA(Config-if-Vlan100)#ip add 192.168.100.1 255.255.255.0
SwitchA(Config-if-Vlan100)#no shut
SwitchA(Config-Vlan100)#exit
```

步骤 9：查看交换机 A 接口上的 IP 地址配置情况。

```
SwitchA#show ip int brief
Index     Interface         IP-Address      Status              Protocol
2002      Loopback          127.0.0.1        up                   up
2004      Vlan10           192.168.10.1      up                   up
2005      Vlan100          192.168.100.1     up                   up

SwitchA#
```

步骤 10：在交换机 B 接口上配置 IP 地址。

```
SwitchB(config)#int vlan 20
SwitchB(Config-if-Vlan20)#ip add 192.168.20.1 255.255.255.0
SwitchB(Config-if-Vlan20)#no shut
SwitchB(Config-Vlan20)#exit
SwitchB(config)#int vlan 100
SwitchB(Config-if-Vlan100)#ip add 192.168.100.2 255.255.255.0
SwitchB(Config-if-Vlan100)#no shut
SwitchB(Config-Vlan40)#exit
```

步骤 11：查看交换机 B 接口上的 IP 地址配置情况。

```
SwitchB#show ip int brief
Index     Interface           IP-Address    Status              Protocol
2002      Loopback            127.0.0.1       up                   up
2004      Vlan20             192.168.20.1     up                   up
2005      Vlan100            192.168.100.2    up                   up

SwitchB#
```

步骤 12：查看未配置静态路由协议时 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.10.0/24 is directly connected, Vlan10      ！后面显示的是VLAN
C       192.168.100.0/24 is directly connected, Vlan100    ！后面显示的是VLAN
Total routes are : 3 item(s)
SwitchA#
```

步骤 13：查看未配置静态路由协议时 SwitchB 的路由表。

```
SwitchB#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.20.0/24 is directly connected, Vlan20      ！后面显示的是VLAN
C       192.168.100.0/24 is directly connected, Vlan100    ！后面显示的是VLAN
Total routes are : 3 item(s)
SwitchB#
```

步骤 14：配置路由协议前，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络未连通，如图 2-4-2 所示。

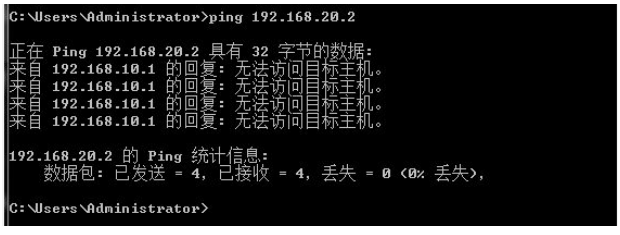


图 2-4-2　连通性测试效果图（一）

（2）在 PC2 上 ping 192.168.10.2，网络未连通，如图 2-4-3 所示。

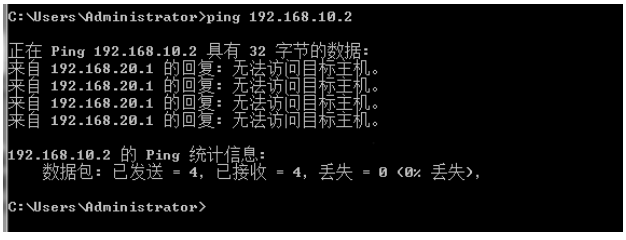


图 2-4-3　连通性测试效果图（二）

步骤 15：在 SwitchA 上配置静态路由。

```
SwitchA#config
SwitchA(config)#ip route 192.168.20.0 255.255.255.0 192.168.100.2
SwitchA#config
```

步骤 16：在 SwitchB 上配置静态路由。

```
SwitchB#config
SwitchB(config)#ip route 192.168.10.0  255.255.255.0  192.168.100.1
SwitchB#config
```

步骤 17：查看配置了静态路由协议的 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.10.0/24 is directly connected, Vlan10    ！后面显示的是VLAN
S       192.168.20.0/24 [1/0] via 192.168.100.2, Vlan100
                                                        ！注意，静态路由的管理距离是1

C       192.168.100.0/24 is directly connected, Vlan100  ！后面显示的是VLAN
Total routes are : 4 item(s)
SwitchA#
```

步骤 18：查看配置了静态路由协议的 SwitchB 的路由表。

```
SwitchB#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
S       192.168.10.0/24 [1/0] via 192.168.100.1, Vlan100
                                    ！注意，静态路由的管理距离是1，后面显示的是VLAN
C       192.168.20.0/24 is directly connected, Vlan20       ！后面显示的是VLAN
C       192.168.100.0/24 is directly connected, Vlan100     ！后面显示的是VLAN
Total routes are : 4 item(s)
SwitchB#
```

步骤 19：配置静态路由协议后，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络已连通，如图 2-4-4 所示。

```
C:\Users\Administrator>ping 192.168.20.2

正在 Ping 192.168.20.2 具有 32 字节的数据:
来自 192.168.20.2 的回复: 字节=32 时间=4ms TTL=126
来自 192.168.20.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.20.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.20.2 的回复: 字节=32 时间=1ms TTL=126

192.168.20.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 4ms, 平均 = 1ms

C:\Users\Administrator>
```

图 2-4-4　连通性测试效果图（三）

（2）在 PC2 上 ping 192.168.10.2，网络已连通，如图 2-4-5 所示。

```
C:\Users\Administrator>ping 192.168.10.2

正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126

192.168.10.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms

C:\Users\Administrator>
```

图 2-4-5　连通性测试效果图（四）

知识拓展

默认路由实现网络连通所需设备如下：

（1）DCR-1751 路由器 2 台。

（2）PC2 台。

（3）Console 配置线 1 条。

（4）交叉线 3 条。

实验拓扑结构如图 2-4-6 所示。

交换机和 PC 的 IP 地址网络参数设置见表 2-4-2。

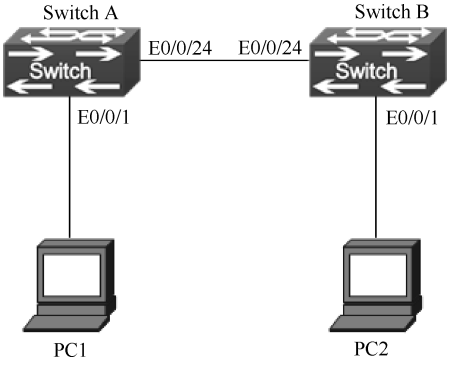


图 2-4-6　实验拓扑结构

表 2-4-2　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
SwitchA 的 VLAN10	E0/0/1	192.168.10.1	255.255.255.0	无
SwitchA 的 VLAN100	E0/0/24	192.168.100.1	255.255.255.0	无
SwitchB 的 VLAN20	E0/0/1	192.168.20.1	255.255.255.0	无
SwitchB 的 VLAN100	E0/0/24	192.168.100.2	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

步骤 1：按照图 2-4-6 连接网络拓扑结构。

步骤 2：按照表 2-4-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          ! 进入特权配置模式
switch#set default                                     ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 4：在交换机 A 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchA
SwitchA(config)#vlan 10
SwitchA(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
SwitchA(Config-Vlan10)#exit
SwitchA(config)#vlan 100
SwitchA(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchA(Config-Vlan100)#exit
SwitchA(config)#
```

步骤 5：查看交换机 A 上的 VLAN。

```
SwitchA#show vlan
VLAN Name        Type      Media     Ports
---- ----------- ---------- --------- ---------------------------------
1    default     Static    ENET      Ethernet0/0/2      Ethernet0/0/3
                                     Ethernet0/0/4      Ethernet0/0/5
                                     Ethernet0/0/6      Ethernet0/0/7
                                     Ethernet0/0/8      Ethernet0/0/9
                                     Ethernet0/0/10     Ethernet0/0/11
                                     Ethernet0/0/12     Ethernet0/0/13
                                     Ethernet0/0/14     Ethernet0/0/15
                                     Ethernet0/0/16     Ethernet0/0/17
                                     Ethernet0/0/18     Ethernet0/0/19
                                     Ethernet0/0/20     Ethernet0/0/21
                                     Ethernet0/0/22     Ethernet0/0/23
                                     Ethernet0/0/25     Ethernet0/0/26
                                     Ethernet0/0/27     Ethernet0/0/28
10   VLAN0010    Static    ENET      Ethernet0/0/1
100  VLAN0100    Static    ENET      Ethernet0/0/24
SwitchA#
```

步骤 6：在交换机 B 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
```

```
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchB
SwitchB(config)#vlan 20
SwitchA(Config-Vlan20)#exit
SwitchB(Config-Vlan20)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
SwitchB(config)#vlan 100
SwitchB(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchB(Config-Vlan100)#exit
SwitchB(config)#
```

步骤 7：查看交换机 B 上的 VLAN。

```
SwitchB#show vlan
VLAN Name        Type      Media     Ports
---- ------------ ---------- --------- ----------------------------------
1    default     Static    ENET    Ethernet0/0/2      Ethernet0/0/3
                                   Ethernet0/0/4      Ethernet0/0/5
                                   Ethernet0/0/6      Ethernet0/0/7
                                   Ethernet0/0/8      Ethernet0/0/9
                                   Ethernet0/0/10     Ethernet0/0/11
                                   Ethernet0/0/12     Ethernet0/0/13
                                   Ethernet0/0/14     Ethernet0/0/15
                                   Ethernet0/0/16     Ethernet0/0/17
                                   Ethernet0/0/18     Ethernet0/0/19
                                   Ethernet0/0/20     Ethernet0/0/21
                                   Ethernet0/0/22     Ethernet0/0/23
                                   Ethernet0/0/25     Ethernet0/0/26
                                   Ethernet0/0/27     Ethernet0/0/28
20   VLAN0020    Static    ENET    Ethernet0/0/1
100  VLAN0100    Static    ENET    Ethernet0/0/24
SwitchB#
```

步骤 8：在交换机 A 接口上配置 IP 地址。

```
SwitchA(config)#int vlan 10
SwitchA(Config-if-Vlan10)#ip add 192.168.10.1 255.255.255.0
SwitchA(Config-if-Vlan10)#no shut
SwitchA(Config-Vlan10)#exit
SwitchA(config)#int vlan 100
SwitchA(Config-if-Vlan100)#ip add 192.168.100.1 255.255.255.0
SwitchA(Config-if-Vlan100)#no shut
SwitchA(Config-Vlan100)#exit
```

步骤 9：查看交换机 A 的接口 IP 地址配置情况。

```
SwitchA#show ip int brief
Index    Interface           IP-Address     Status              Protocol
2002     Loopback            127.0.0.1        up                  up
```

```
2004     Vlan10              192.168.10.1     up                  up
2005     Vlan100             192.168.100.1    up                  up

SwitchA#
```

步骤 10：在交换机 B 接口上配置 IP 地址。

```
SwitchB(config)#int vlan 20
SwitchB(Config-if-Vlan20)#ip add 192.168.20.1 255.255.255.0
SwitchB(Config-if-Vlan20)#no shut
SwitchB(Config-Vlan20)#exit
SwitchB(config)#int vlan 100
SwitchB(Config-if-Vlan100)#ip add 192.168.100.2 255.255.255.0
SwitchB(Config-if-Vlan100)#no shut
SwitchB(Config-Vlan40)#exit
```

步骤 11：查看交换机 B 的接口 IP 地址配置情况。

```
SwitchB#show ip int brief
Index     Interface           IP-Address      Status              Protocol
2002      Loopback            127.0.0.1         up                  up
2004      Vlan20              192.168.20.1      up                  up
2005      Vlan100             192.168.100.2     up                  up
SwitchB#
```

步骤 12：查看未配置默认路由协议交换机 A 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.10.0/24 is directly connected, Vlan10
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 3 item(s)
SwitchA#
```

步骤 13：查看未配置默认路由协议交换机 B 的路由表。

```
SwitchB#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
```

```
C       192.168.20.0/24 is directly connected, Vlan20
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 3 item(s)
SwitchB#
```

步骤 14：配置路由协议前，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络未连通，如图 2-4-7 所示。

图 2-4-7　连通性测试效果图（一）

（2）在 PC2 上 ping 192.168.10.2，网络未连通，如图 2-4-8 所示。

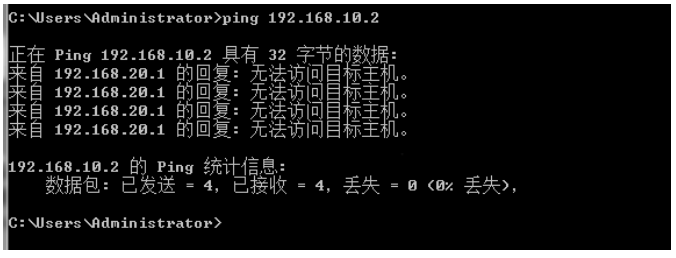


图 2-4-8　连通性测试效果图（二）

步骤 15：在 SwitchA 上配置默认路由。

```
SwitchA#config
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

步骤 16：在 SwitchB 上配置默认路由。

```
SwitchB#config
SwitchA(config)#ip route 0.0.0.0 0.0.0.0  192.168.100.1
```

步骤 17：查看配置了默认路由协议 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is 192.168.100.2 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.2, Vlan100
C       127.0.0.0/8 is directly connected, Loopback
```

```
C       192.168.10.0/24 is directly connected, Vlan10
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchA#
```

步骤 18：查看配置了默认路由协议 SwitchB 的路由表。

```
SwitchB#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is 192.168.100.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.1, Vlan100
C       127.0.0.0/8 is directly connected, Loopback
C       192.168.20.0/24 is directly connected, Vlan20
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchB#
```

步骤 19：配置路由协议后，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络已连通，如图 2-4-9 所示。

图 2-4-9　连通性测试效果图（三）

（2）在 PC2 上 ping 192.168.10.2，网络已连通，如图 2-4-10 所示。

图 2-4-10　连通性测试效果图（四）

学习小结

本学习活动介绍了三层交换机之间如何实现静态路由，需要注意的是添加静态路由时非直连网段也要进行配置。静态路由开销小，但不灵活，只适用于相对稳定的网络。在小型网络环境中，选择静态路由是可以的，但对于中大型网络而言，静态路由的工作量就很大了。

学习活动 2　交换机间的 RIP 动态路由配置

RIP 是应用较早、使用较普遍的动态路由协议，也是内部网关协议，由于 RIP 跳数作为衡量路径的开销，且规定最大跳数为 15，因此 RIP 在实际应用中还是有一定限制的，通常适用于中小型的企业网络。

学习情境

随着公司规模的不断扩大，网络设备的数量增多了。公司的网络管理员发现原有的静态路由已经不适合现在的公司。因此，决定在公司的交换机之间使用动态的 RIP 路由协议，实现网络的互连。

情境分析

由于公司的网络规模开始扩大，管理员发现使用静态路由确实不合适了，所以决定使用动态的 RIP 路由协议。

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）PC 4 台。

（3）交叉线 1 条。

（4）直连线 4 条。

RIP 路由协议拓扑结构如图 2-4-11 所示。

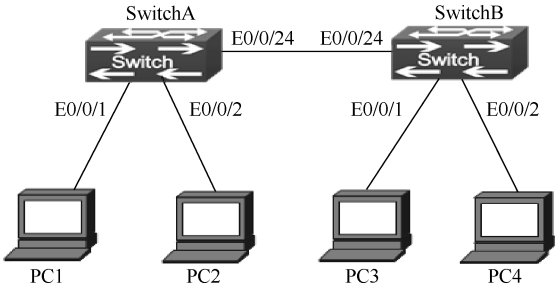


图 2-4-11　RIP 路由协议拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 2-4-3。

表 2-4-3　交换机和 PC 的 IP 地址网络参数设置

设　　备	端　　口	IP 地址	子网掩码	网　　关
SwitchA 的 VLAN10	E0/0/1	192.168.0.1	255.255.255.0	无
SwitchA 的 VLAN20	E0/0/2	192.168.1.1	255.255.255.0	无
SwitchA 的 VLAN100	E0/0/24	192.168.100.1	255.255.255.0	无
SwitchB 的 VLAN30	E0/0/1	192.168.2.1	255.255.255.0	无
SwitchB 的 VLAN40	E0/0/1	192.168.3.1	255.255.255.0	无
SwitchB 的 VLAN100	E0/0/24	192.168.100.2	255.255.255.0	无
PC1	E0/0/1	192.168.0.2	255.255.255.0	192.168.0.1
PC2	E0/0/2	192.168.1.2	255.255.255.0	192.168.1.1
PC3	E0/0/1	192.168.2.2	255.255.255.0	192.168.2.1
PC4	E0/0/2	192.168.3.2	255.255.255.0	192.168.3.1

相关知识

RIP（Routing Information Protocol，路由信息协议）是应用较早、使用较普遍的内部网关协议（Interior Gateway Protocol，IGP），适用于小型同类网络的一个自治系统（Autonomous System，AS）内的路由信息的传递。RIP 是基于距离矢量算法的。它使用“跳数”，即 metric 来衡量到达目的地址的路由距离，取值为 1～15，数值 16 表示无穷大。RIP 进程使用 UDP 的 520 端口来发送和接收 RIP 分组。RIP 分组每隔 30s 以广播的形式发送一次，为了防止出现“广播风暴”，其后续分组将做随机延时后发送。在 RIP 中，如果一个路由在 180s 内未被刷新，则相应的距离被设定成无穷大，并从路由表中删除该表项。

使用距离矢量路由协议的路由器并不了解到达目的网络的整条路径。距离矢量协议将路由器作为通往最终目的地的路径上的路标。路由器唯一了解的远程网络信息就是到该网络的距离（即度量）以及可通过哪条路径或哪个接口到达该网络。 距离矢量路由协议并不了解确切的网络拓扑图。

有两个距离矢量 IPv4 IGP，即 RIPv1 —— 第一代传统协议，RIPv2 —— 简单距离矢量路由协议。

RIPv1 被提出较早，其中有许多缺陷。为了改善 RIPv1 的不足，在 RFC 1388 中提出了改进的 RIPv2，并在 RFC 1723 和 RFC 2453 中进行了修订。RIPv2 定义了一套有效的改进方案，新的 RIPv2 支持子网路由选择，支持 CIDR，支持组播，并提供了验证机制。其区别见表 2-4-4。

表 2-4-4　RIPv1 和 RIPv2 的区别

RIPv1	RIPv2
有类路由协议	无类路由协议
不能支持 VLSM	可以支持 VLSM
没有认证的功能	可以支持认证，并且有明文和 MD5 两种认证

续表

RIPv1	RIPv2
手工汇总的功能	可以在关闭自动汇总的前提下，进行手工汇总
广播更新 255.255.255.255	组播更新 224.0.0.9

在三层交换机上 RIP 动态路由协议的配置命令如下：

```
Switch#config
Switch(config)# router rip              !启动RIP路由协议
Switch(config-router)#network vlan ID  !宣告路由器的VLAN
Switch(config-router)#
```

步骤实现

步骤 1：按照图 2-4-11 连接网络拓扑结构图。

步骤 2：按照表 2-4-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          ! 进入特权配置模式
switch#set default                                     ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 4：在交换机 A 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchA
SwitchA(config)#vlan 10
SwitchA(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
SwitchA(Config-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(Config-Vlan20)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 20 successfully
SwitchA(Config-Vlan20)#exit
SwitchA(config)#vlan 100
SwitchA(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchA(Config-Vlan100)#exit
SwitchA(config)#
```

步骤 5：在交换机 B 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
```

```
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchB
SwitchB(config)#vlan 30
SwitchB(config-Vlan30)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
SwitchB(config-Vlan30)#exit
SwitchB(config)#vlan 40
SwitchB(config-Vlan40)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 40 successfully
SwitchB(config-Vlan40)#exit
SwitchB(config)#vlan 100
SwitchB(config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchB(config-Vlan100)#exit
SwitchB(config)#
```

步骤 6：在交换机 A 接口上配置 IP 地址。

```
SwitchA(config)#int vlan 10
SwitchA(config-if-Vlan10)#ip add 192.168.0.1 255.255.255.0
SwitchA(config-if-Vlan10)#no shut
SwitchA(config-Vlan10)#exit
SwitchA(config)#int vlan 20
SwitchA(config-if-Vlan20)#ip add 192.168.1.1 255.255.255.0
SwitchA(config-if-Vlan20)#no shut
SwitchA(config-Vlan20)#exit
SwitchA(config)#int vlan 100
SwitchA(config-if-Vlan100)#ip add 192.168.100.1 255.255.255.0
SwitchA(config-if-Vlan100)#no shut
SwitchA(config-Vlan100)#exit
```

步骤 7：查看 SwitchA 的接口 IP 地址配置情况。

```
SwitchA #sho ip interface brief
Index    Interface           IP-Address    Status            Protocol
2002     Loopback            127.0.0.1     up                up
2004     Vlan10              192.168.0.1   up                up
2005     Vlan20              192.168.1.1   up                up
2006     Vlan100             192.168.100.1 up                up
SwitchA #
```

步骤 8：在交换机 B 接口上配置 IP 地址。

```
SwitchB(config)#int vlan 30
SwitchB(Config-if-Vlan30)#ip add 192.168.2.1 255.255.255.0
SwitchB(Config-if-Vlan30)#no shut
SwitchB(Config-Vlan30)#exit
SwitchB(config)#int vlan 40
SwitchB(Config-if-Vlan40)#ip add 192.168.3.1 255.255.255.0
SwitchB(Config-if-Vlan40)#no shut
```

```
SwitchB(Config-Vlan40)#exit
SwitchB(config)#int vlan 100
SwitchB(Config-if-Vlan100)#ip add 192.168.100.2 255.255.255.0
SwitchB(Config-if-Vlan100)#no shut
SwitchB(Config-Vlan40)#exit
```

步骤 9：查看 SwitchB 的接口 IP 地址配置情况。

```
SwitchB#show ip interface brief
Index    Interface           IP-Address    Status            Protocol
2002     Loopback            127.0.0.1     up                up
2004     Vlan30              192.168.2.1   up                up
2005     Vlan40              192.168.3.1   up                up
2006     Vlan100             192.168.100.2 up                up
SwitchA#
```

步骤 10：查看未配置 RIP 路由协议的 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.0.0/24 is directly connected, Vlan10
C       192.168.1.0/24 is directly connected, Vlan20
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchA#
```

步骤 11：查看未配置 RIP 路由协议的 SwitchB 的路由表。

```
SwitchB#sho ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.2.0/24 is directly connected, Vlan30
C       192.168.3.0/24 is directly connected, Vlan40
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchB#
```

步骤 12：配置路由协议前，同一个交换机的 VLAN 可以通信，不同交换机的 VLAN 无

法通信，如图 2-4-12 所示。

图 2-4-12　连通性测试效果图（一）

步骤 13：在 SwitchA 上配置 RIP 路由协议。

```
SwitchA#config
SwitchA(config)# router rip                    ！启动RIP路由协议
SwitchA(config-router)#version 1               ！设置版本号
SwitchA(config-router)#network vlan 10         ！宣告VLAN
SwitchA(config-router)#network vlan 20
SwitchA(config-router)#network vlan 100
SwitchA(config-router)#
```

步骤 14：在 SwitchB 上配置 RIP 路由协议。

```
SwitchB#config
SwitchB(config)# router rip
SwitchB(config)#version 1
SwitchB(config-router)#network vlan 30
SwitchB(config-router)#network vlan 40
SwitchB(config-router)#network vlan 100
SwitchB(config-router)#
```

步骤 15：查看配置了 RIP 路由协议的 SwitchA 的路由表。

```
SwitchA #sho ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.0.0/24 is directly connected, Vlan10
C       192.168.1.0/24 is directly connected, Vlan20
```

```
R      192.168.2.0/24 [120/2] via 192.168.100.2, Vlan100, 00:00:47
R      192.168.3.0/24 [120/2] via 192.168.100.2, Vlan100, 00:00:47
C      192.168.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
SwitchA #
```

步骤 16：查看配置了 RIP 路由协议的 SwitchB 的路由表。

```
SwitchB #sho ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
R      192.168.0.0/24 [120/2] via 192.168.100.1, Vlan100, 00:00:06
R      192.168.1.0/24 [120/2] via 192.168.100.1, Vlan100, 00:00:06
C      192.168.2.0/24 is directly connected, Vlan30
C      192.168.3.0/24 is directly connected, Vlan40
C      192.168.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
SwitchB #
```

步骤 17：配置了 RIP 协议后，验证网络的连通性，如图 2-4-13 所示。

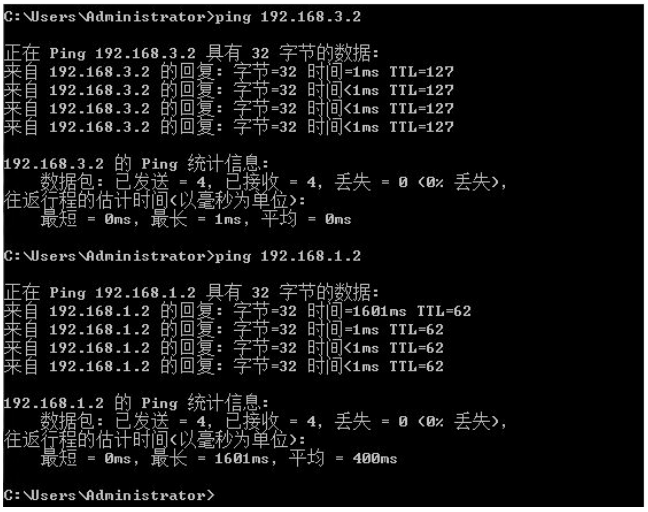


图 2-4-13　连通性测试效果图（二）

小贴士

神州数码的交换机在实现 RIP 路由协议时，宣告的是 VLAN 号。这点和其他厂商的设备不太一样，且默认的版本号为 2，要特别注意。例如:

```
SwitchA(config)# router rip
```

```
SwitchA(config-router)#version 1
SwitchA(config-router)#network vlan 10          !VLAM的ID
SwitchA(config-router)#network vlan 20          !VLAM的ID
SwitchA(config-router)#network vlan 100         !VLAM的ID
```

知识拓展

RIPv2 动态路由协议实现时所需设备如下：

（1）DCRS-5650 交换机 2 台。

（2）PC 4 台。

（3）交叉线 1 条。

（4）直连线 4 条。

RIPv2 路由协议拓扑结构如图 2-4-14 所示。交换机和 PC 的 IP 地址网络参数设置见表 2-4-5。

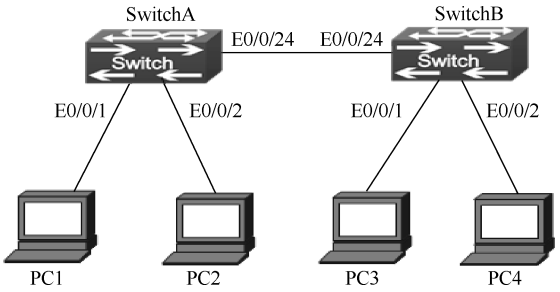


图 2-4-14　RIPv2 路由协议拓扑结构

表 2-4-5　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
SwitchA 的 VLAN10	E0/0/1	172.16.0.1	255.255.255.0	无
SwitchA 的 VLAN20	E0/0/2	172.16.1.1	255.255.255.0	无
SwitchA 的 VLAN100	E0/0/24	172.16.100.1	255.255.255.0	无
SwitchB 的 VLAN30	E0/0/1	172.16.2.1	255.255.255.0	无
SwitchB 的 VLAN40	E0/0/1	172.16.3.1	255.255.255.0	无
SwitchB 的 VLAN100	E0/0/24	172.16.100.2	255.255.255.0	无
PC1	E0/0/1	172.16.0.2	255.255.255.0	172.16.0.1
PC2	E0/0/2	172.16.1.2	255.255.255.0	172.16.1.1
PC3	E0/0/1	172.16.2.2	255.255.255.0	172.16.2.1
PC4	E0/0/2	172.16.3.2	255.255.255.0	172.16.3.1

步骤 1：按照图 2-4-14 连接网络拓扑结构。

步骤 2：按照表 2-4-5 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                   !进入特权配置模式
```

```
switch#set default                                    !恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                         !重启交换机
Process with reboot? [Y/N]y
```

步骤 4：在交换机 A 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchA
SwitchA(config)#vlan 10
SwitchA(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
SwitchA(Config-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(Config-Vlan20)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 20 successfully
SwitchA(Config-Vlan20)#exit
SwitchA(config)#vlan 100
SwitchA(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchA(Config-Vlan100)#exit
SwitchA(config)#
```

步骤 5：在交换机 B 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchB
SwitchB(config)#vlan 30
SwitchB(Config-Vlan30)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
SwitchB(Config-Vlan30)#exit
SwitchB(config)#vlan 40
SwitchB(Config-Vlan40)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 40 successfully
SwitchB(Config-Vlan40)#exit
SwitchB(config)#vlan 100
SwitchB(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchB(Config-Vlan100)#exit
SwitchB(config)#
```

步骤 6：在交换机 A 接口上配置 IP 地址。

```
SwitchA(config)#int vlan 10
SwitchA(Config-if-Vlan10)#ip add 172.16.0.1 255.255.255.0
```

```
SwitchA(Config-if-Vlan10)#no shut
SwitchA(Config-Vlan10)#exit
SwitchA(config)#int vlan 20
SwitchA(Config-if-Vlan20)#ip add 172.16.1.1 255.255.255.0
SwitchA(Config-if-Vlan20)#no shut
SwitchA(Config-Vlan20)#exit
SwitchA(config)#int vlan 100
SwitchA(Config-if-Vlan100)#ip add 172.16.100.1 255.255.255.0
SwitchA(Config-if-Vlan100)#no shut
SwitchA(Config-Vlan100)#exit
```

步骤 7：查看交换机 A 的接口 IP 地址配置情况。

```
SwitchA#show ip int brief
Index    Interface            IP-Address      Status              Protocol
2002     Loopback             127.0.0.1         up                  up
2004     Vlan10               172.16.0.1        up                  up
2005     Vlan20               172.16.1.1        up                  up
2006     Vlan100              172.16.100.1      up                  up
SwitchA#
```

步骤 8：在交换机 B 接口上配置 IP 地址。

```
SwitchB(config)#int vlan 30
SwitchB(Config-if-Vlan30)#ip add 172.16.2.1 255.255.255.0
SwitchB(Config-if-Vlan30)#no shut
SwitchB(Config-Vlan30)#exit
SwitchB(config)#int vlan 40
SwitchB(Config-if-Vlan40)#ip add 172.16.3.1 255.255.255.0
SwitchB(Config-if-Vlan40)#no shut
SwitchB(Config-Vlan40)#exit
SwitchB(config)#int vlan 100
SwitchB(Config-if-Vlan100)#ip add 172.16.100.2 255.255.255.0
SwitchB(Config-if-Vlan100)#no shut
SwitchB(Config-Vlan40)#exit
```

步骤 9：查看交换机 B 的接口 IP 地址配置情况。

```
SwitchB#show ip int brief
Index    Interface            IP-Address      Status              Protocol
2002     Loopback             127.0.0.1           up                  up
2004     Vlan30               172.16.2.1          up                  up
2005     Vlan40               172.16.3.1          up                  up
2006     Vlan100              172.16.100.2        up                  up


SwitchB#
```

步骤 10：查看未配置 RIPv2 路由协议的 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      172.16.0.0/24 is directly connected, Vlan10
C      172.16.1.0/24 is directly connected, Vlan20
C      172.16.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchA#
```

步骤 11：查看未配置 RIPv2 路由协议的 SwitchB 的路由表。

```
SwitchB#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      172.16.2.0/24 is directly connected, Vlan30
C      172.16.3.0/24 is directly connected, Vlan40
C      172.16.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchB#
```

步骤 12：配置路由协议前，同一个交换机的 VLAN 可以通信，不同交换机的 VLAN 无法通信，如图 2-4-15 所示。

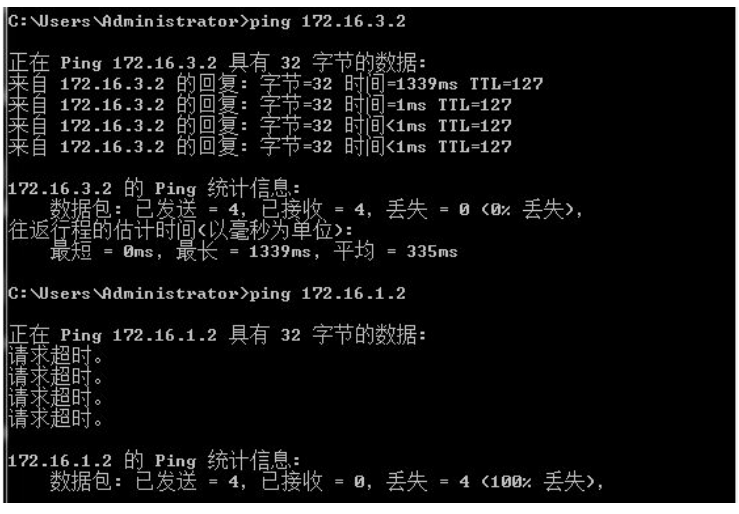


图 2-4-15　连通性测试效果图（一）

步骤 13：在 SwitchA 上配置 RIP 路由协议。

```
SwitchA#config
SwitchA(config)# router  rip
SwitchA(config-router)#network vlan 10
SwitchA(config-router)#network vlan 20
SwitchA(config-router)#network vlan 100
SwitchA(config-router)#
```

步骤 14：在 SwitchB 上配置 RIP 路由协议。

```
SwitchB#config
SwitchB(config)# router rip
SwitchB(config-router)#network vlan 30
SwitchB(config-router)#network vlan 40
SwitchB(config-router)#network vlan 100
SwitchB(config-router)#
```

步骤 15：查看配置了 RIPv2 路由协议的 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       172.16.0.0/24 is directly connected, Vlan10
C       172.16.1.0/24 is directly connected, Vlan20
R       172.16.2.0/24 [120/2] via 172.16.100.2, Vlan100, 00:00:15
R       172.16.3.0/24 [120/2] via 172.16.100.2, Vlan100, 00:00:15
C       172.16.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
SwitchA#
```

步骤 16：查看配置了 RIPv2 路由协议的 SwitchB 的路由表。

```
SwitchB#show ip route
sho ip ro
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
R       172.16.0.0/24 [120/2] via 172.16.100.1, Vlan100, 00:00:42
R       172.16.1.0/24 [120/2] via 172.16.100.1, Vlan100, 00:00:42
C       172.16.2.0/24 is directly connected, Vlan30
```

```
C       172.16.3.0/24 is directly connected, Vlan40
C       172.16.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
SwitchB#
```

步骤 17：配置了 RIP 协议后，验证网络的连通性，如图 2-4-16 所示。

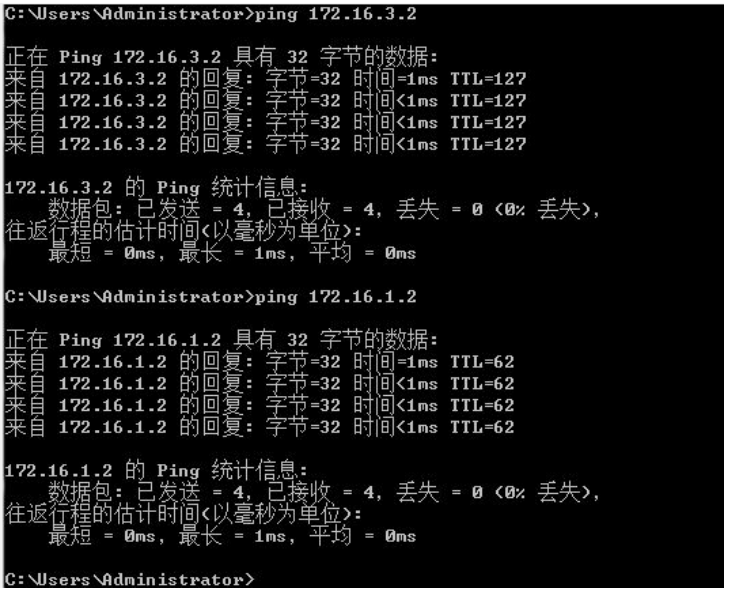


图 2-4-16　连通性测试效果图（二）

学习小结

本学习活动介绍了交换机之间如何实现 RIP 路由，需要注意的是 RIP 协议有两个版本——RIPv1 和 RIPv2，no auto-summary 功能只支持 RIPv2。宣告时只宣告自己的直连 VLAN，实现动态更新路由。

学习活动 3　交换机间的 OSPF 路由配置

OSPF（Open Shortest Path First，开放式最短路径优先）协议是目前网络中应用最广泛的动态路由协议之一，也属于内部网关路由协议，能够适应各种规模的网络环境，是典型的链路状态（Link State）协议。

学习情境

公司的规模越来越大，网络设备的数量也逐渐增多，该公司的网络管理员想使用动态的 OSPF 路由协议实现网络的互连。

情境分析

由于公司的网络规模越来越大，管理员发现使用 OSPF 路由协议非常适用，因为 OSPF 路由协议可以实现快速的收敛，并且出现环路的可能性不大，适用于中大型企业网络。

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）PC 4 台。

（3）交叉线 1 条。

（4）Console 配置线 1 条。

（5）直连线 4 条。

OSPF 单区域路由协议拓扑结构如图 2-4-17 所示。

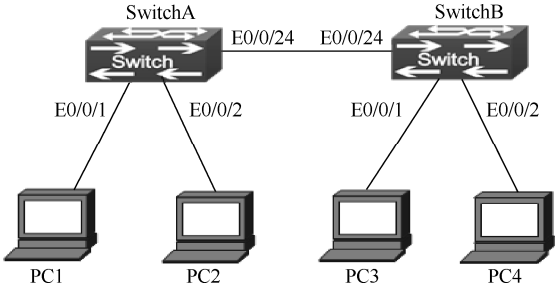


图 2-4-17　OSPF 单区域路由协议拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 2-4-6。

表 2-4-6　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
SwitchA 的 VLAN10	E0/0/1	192.168.0.1	255.255.255.0	无
SwitchA 的 VLAN20	E0/0/2	192.168.1.1	255.255.255.0	无
SwitchA 的 VLAN100	E0/0/24	192.168.100.1	255.255.255.0	无
SwitchB 的 VLAN30	E0/0/1	192.168.2.1	255.255.255.0	无
SwitchB 的 VLAN40	E0/0/1	192.168.3.1	255.255.255.0	无
SwitchB 的 VLAN100	E0/0/24	192.168.100.2	255.255.255.0	无
PC1	E0/0/1	192.168.0.2	255.255.255.0	192.168.0.1
PC2	E0/0/2	192.168.1.2	255.255.255.0	192.168.1.1
PC3	E0/0/1	192.168.2.2	255.255.255.0	192.168.2.1
PC4	E0/0/2	192.168.3.2	255.255.255.0	192.168.3.1

相关知识

OSPF 是 IETF 组织开发的一个基于 LS 的自治系统内部路由协议。其特性如下：

（1）适应范围广 —— 支持各种规模的网络，最多可支持几百台路由器。

（2）收敛快速——在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。

（3）无自环——OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。

（4）区域划分管理——允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。

（5）路由分级——使用 4 类不同等级的路由，按优先顺序来说分别如下：区域内路由、区域间路由、第一类外部路由、第二类外部路由。

（6）支持验证——支持基于接口的报文验证以保证路由计算的安全性。

（7）可以多播发送——在有多播发送能力的链路层上以多播地址收发报文，既达到了广播的作用，又最大限度地减小对其他网络的干扰。

OSPF 路由协议通过向全网通告自己的路由信息，使网络中每台设备最终同步一个具有全网链路状态的数据库（LSDB），然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

在大型的网络环境中，OSPF 支持区域的划分，以对网络进行合理规划。划分区域时必须存在 area0（骨干区域）。其他区域和骨干区域直接相连，或通过虚链路的方式连接。

要创建 OSPF 路由进程，在全局命令配置模式下执行以下命令：

```
Switch#config
Switch(config)#router ospf process-id    !启动OSPF路由进程
Switch(config-router)#network network netmask area area-id
!定义接口所属区域
Switch(config-router)#
```

说明：在神州数码交换机中，在使用 OSPF 路由协议时，进程 ID 可以省略，network 后面跟的是直连网段和相应的子网掩码，不能写成反码，配置成功后，交换机会自动转换为反码显示，这一点和其他品牌的交换机有所区别，需要特别注意。

步骤实现

步骤 1：按照图 2-4-17 连接网络拓扑结构。

步骤 2：按照表 2-4-6 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          !进入特权配置模式
switch#set default                                     !恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          !重启交换机
Process with reboot? [Y/N]y
```

步骤 4：在 SwitchA 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
```

```
DCRS-5650-28(config)#hostname  SwitchA
SwitchA(config)#vlan 10
SwitchA(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
SwitchA(Config-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(Config-Vlan20)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 20 successfully
SwitchA(Config-Vlan20)#exit
SwitchA(config)#vlan 100
SwitchA(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchA(Config-Vlan100)#exit
SwitchA(config)#
```

步骤 5：在 SwitchB 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchB
SwitchB(config)#vlan 30
SwitchB(Config-Vlan30)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
SwitchB(Config-Vlan30)#exit
SwitchB(config)#vlan 40
SwitchB(Config-Vlan40)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 40 successfully
SwitchB(Config-Vlan40)#exit
SwitchB(config)#vlan 100
SwitchB(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchB(Config-Vlan100)#exit
SwitchB(config)#
```

步骤 6：在 SwitchA 上配置接口 IP 地址。

```
SwitchA(config)#int vlan 10
SwitchA(Config-if-Vlan10)#ip add 192.168.0.1 255.255.255.0
SwitchA(Config-if-Vlan10)#no shut
SwitchA(Config-Vlan10)#exit
SwitchA(config)#int vlan 20
SwitchA(Config-if-Vlan20)#ip add 192.168.1.1 255.255.255.0
SwitchA(Config-if-Vlan20)#no shut
SwitchA(Config-Vlan20)#exit
SwitchA(config)#int vlan 100
SwitchA(Config-if-Vlan100)#ip add 192.168.100.1 255.255.255.0
SwitchA(Config-if-Vlan100)#no shut
```

```
SwitchA(Config-Vlan100)#exit
```

步骤 7：查看 SwitchA 的 IP 地址配置情况。

```
SwitchA #show ip interface brief
Index    Interface          IP-Address    Status            Protocol
2002     Loopback           127.0.0.1      up                 up
2004     Vlan10             192.168.0.1    up                 up
2005     Vlan20             192.168.1.1    up                 up
2006     Vlan100            192.168.100.1   up                up

SwitchA #
```

步骤 8：在 SwitchB 上配置接口 IP 地址。

```
SwitchB(config)#int vlan 30
SwitchB(Config-if-Vlan30)#ip add 192.168.2.1 255.255.255.0
SwitchB(Config-if-Vlan30)#no shut
SwitchB(Config-Vlan30)#exit
SwitchB(config)#int vlan 40
SwitchB(Config-if-Vlan40)#ip add 192.168.3.1 255.255.255.0
SwitchB(Config-if-Vlan40)#no shut
SwitchB(Config-Vlan40)#exit
SwitchB(config)#int vlan 100
SwitchB(Config-if-Vlan100)#ip add 192.168.100.2 255.255.255.0
SwitchB(Config-if-Vlan100)#no shut
SwitchB(Config-Vlan100)#exit
SwitchB(Config)#
```

步骤 9：查看 SwitchB 的 IP 地址配置情况。

```
SwitchB #show ip interface brief
Index    Interface          IP-Address    Status        Protocol
2002     Loopback           127.0.0.1       up            up
2004     Vlan30             192.168.2.1     up            up
2005     Vlan40             192.168.3.1     up            up
2006     Vlan100            192.168.100.2   up            up

SwitchB #
```

步骤 10：查看 SwitchA 的路由表。

```
SwitchA #show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.0.0/24 is directly connected, Vlan10
```

```
C      192.168.1.0/24 is directly connected, Vlan20
C      192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchA #
```

步骤 11：查看 SwitchB 的路由表。

```
SwitchB #show  ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      192.168.2.0/24 is directly connected, Vlan30
C      192.168.3.0/24 is directly connected, Vlan40
C      192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchB #
```

步骤 12：配置路由协议前，同一个交换机的 VLAN 可以通信，不同交换机的 VLAN 无法通信，如图 2-4-18 所示。

图 2-4-18　连通性测试效果图（一）

步骤 13：在 SwitchA 上配置 OSPF 路由协议。

```
SwitchA#config
SwitchA(config)#router ospf 1
SwitchA(config-router)#network 192.168.0.0 0.0.0.255 area 0
SwitchA(config-router)#network 192.168.1.0 0.0.0.255 area 0
SwitchA(config-router)#network 192.168.100.0 0.0.0.255 area 0
SwitchA(config-router)#
```

步骤 14：在 SwitchB 上配置 OSPF 路由协议。

```
SwitchB#config
SwitchB(config)#router ospf 1
SwitchB(config-router)#network 192.168.2.0 0.0.0.255 area 0
SwitchB(config-router)#network 192.168.3.0 0.0.0.255 area 0
SwitchB(config-router)#network 192.168.100.0 0.0.0.255 area 0
SwitchB(config-router)#
```

步骤 15：查看 SwitchA 的路由表。

```
sw-1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
C       192.168.0.0/24 is directly connected, Vlan10
C       192.168.1.0/24 is directly connected, Vlan20
O       192.168.2.0/24 [110/20] via 192.168.100.2, Vlan100, 00:00:06
O       192.168.3.0/24 [110/20] via 192.168.100.2, Vlan100, 00:00:06
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
sw-1#
```

步骤 16：查看 SwitchB 的路由表。

```
sw-2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
O       192.168.0.0/24 [110/20] via 192.168.100.1, Vlan100, 00:00:28
O       192.168.1.0/24 [110/20] via 192.168.100.1, Vlan100, 00:00:28
C       192.168.2.0/24 is directly connected, Vlan30
C       192.168.3.0/24 is directly connected, Vlan40
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
sw-2#
```

步骤 17：配置了 OSPF 单区域协议后，验证网络的连通性，如图 2-4-19 所示。

```
C:\Users\Administrator>ping 192.168.3.2

正在 Ping 192.168.3.2 具有 32 字节的数据:
来自 192.168.3.2 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.3.2 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.3.2 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.3.2 的回复: 字节=32 时间<1ms TTL=127

192.168.3.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间=1601ms TTL=62
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=62

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1601ms, 平均 = 400ms

C:\Users\Administrator>
```

图 2-4-19　连通性测试效果图（二）

知识拓展

OSPF 动态路由协议多区域实现时所需设备如下：

（1）DCRS-5650 交换机 2 台。

（2）PC 4 台。

（3）交叉线 1 条。

（4）直连线 4 条。

OSPF 多区域路由协议拓扑结构如图 2-4-20 所示。

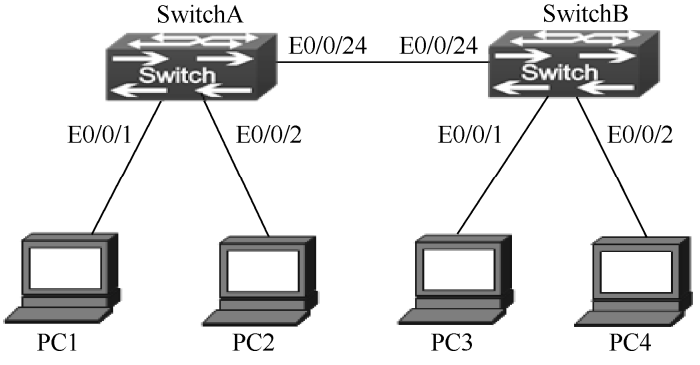


图 2-4-20 OSPF 多区域路由协议拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 2-4-7。

表 2-4-7　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP	子网掩码	网　关
SwitchA 的 VLAN10	E0/0/1	192.168.0.1	255.255.255.0	无
SwitchA 的 VLAN20	E0/0/2	192.168.1.1	255.255.255.0	无
SwitchA 的 VLAN100	E0/0/24	192.168.100.1	255.255.255.0	无
SwitchB 的 VLAN30	E0/0/1	192.168.2.1	255.255.255.0	无
SwitchB 的 VLAN40	E0/0/1	192.168.3.1	255.255.255.0	无
SwitchB 的 VLAN100	E0/0/24	192.168.100.2	255.255.255.0	无
PC1	E0/0/1	192.168.0.2	255.255.255.0	192.168.0.1
PC2	E0/0/2	192.168.1.2	255.255.255.0	192.168.1.1
PC3	E0/0/1	192.168.2.2	255.255.255.0	192.168.2.1
PC4	E0/0/2	192.168.3.2	255.255.255.0	192.168.3.1

步骤 1：按照图 2-4-20 连接网络拓扑结构。

步骤 2：按照表 2-4-7 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          ! 进入特权配置模式
switch#set default                                     ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 4：在 SwitchA 上划分 VLAN。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchA
SwitchA(config)#vlan 10
SwitchA(Config-Vlan10)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 10 successfully
SwitchA(Config-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(Config-Vlan20)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 20 successfully
SwitchA(Config-Vlan20)#exit
SwitchA(config)#vlan 100
SwitchA(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchA(Config-Vlan100)#exit
SwitchA(config)#
```

步骤 5：在 SwitchB 上划分 VLAN。

```
DCRS-5650-28>
```

```
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  SwitchB
SwitchB(config)#vlan 30
SwitchB(Config-Vlan30)#switchport interface e0/0/1
Set the port Ethernet0/0/1 access vlan 20 successfully
SwitchB(Config-Vlan30)#exit
SwitchB(config)#vlan 40
SwitchB(Config-Vlan40)#switchport interface e0/0/2
Set the port Ethernet0/0/2 access vlan 40 successfully
SwitchB(Config-Vlan40)#exit
SwitchB(config)#vlan 100
SwitchB(Config-Vlan100)#switchport interface e0/0/24
Set the port Ethernet0/0/24 access vlan 100 successfully
SwitchB(Config-Vlan100)#exit
SwitchB(config)#
```

步骤 6：在 SwitchA 上配置接口 IP 地址。

```
SwitchA(config)#int vlan 10
SwitchA(Config-if-Vlan10)#ip add 192.168.0.1 255.255.255.0
SwitchA(Config-if-Vlan10)#no shut
SwitchA(Config-Vlan10)#exit
SwitchA(config)#int vlan 20
SwitchA(Config-if-Vlan20)#ip add 192.168.1.1 255.255.255.0
SwitchA(Config-if-Vlan20)#no shut
SwitchA(Config-Vlan20)#exit
SwitchA(config)#int vlan 100
SwitchA(Config-if-Vlan100)#ip add 192.168.100.1 255.255.255.0
SwitchA(Config-if-Vlan100)#no shut
SwitchA(Config-Vlan100)#exit
```

步骤 7：查看 SwitchA 的 IP 地址配置情况。

```
SwitchA#show ip interface brief
Index    Interface           IP-Address    Status            Protocol
2002     Loopback            127.0.0.1       up                up
2004     Vlan10              192.168.0.1     up                up
2005     Vlan20              192.168.1.1     up                up
2006     Vlan100             192.168.100.1   up                up

SwitchA#
```

步骤 8：在 SwitchB 上配置接口 IP 地址。

```
SwitchB(config)#int vlan 30
SwitchB(Config-if-Vlan30)#ip add 192.168.2.1 255.255.255.0
SwitchB(Config-if-Vlan30)#no shut
SwitchB(Config-Vlan30)#exit
SwitchB(config)#int vlan 40
```

```
SwitchB(Config-if-Vlan40)#ip add 192.168.3.1 255.255.255.0
SwitchB(Config-if-Vlan40)#no shut
SwitchB(Config-Vlan40)#exit
SwitchB(config)#int vlan 100
SwitchB(Config-if-Vlan100)#ip add 192.168.100.2 255.255.255.0
SwitchB(Config-if-Vlan100)#no shut
SwitchB(Config-Vlan100)#exit
SwitchB(Config)#
```

步骤 9：查看 SwitchB 的 IP 地址配置情况。

```
SwitchB#show ip interface brief
Index    Interface           IP-Address    Status            Protocol
2002     Loopback            127.0.0.1       up                up
2004     Vlan30              192.168.2.1     up                up
2005     Vlan40              192.168.3.1     up                up
2006     Vlan100             192.168.100.2    up                up

SwitchB#
```

步骤 10：查看 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      192.168.0.0/24 is directly connected, Vlan10
C      192.168.1.0/24 is directly connected, Vlan20
C      192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchA#
```

步骤 11：查看 SwitchB 的路由表。

```
SwitchB#show  ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C      127.0.0.0/8 is directly connected, Loopback
C      192.168.2.0/24 is directly connected, Vlan30
C      192.168.3.0/24 is directly connected, Vlan40
```

```
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 4 item(s)
SwitchB#
```

步骤 12：配置路由协议前，同一个交换机的 VLAN 可以通信，不同交换机的 VLAN 无法通信，如图 2-4-21 所示。

图 2-4-21　连通性测试效果图（一）

步骤 13：在 SwitchA 上配置 OSPF 路由协议。

```
SwitchA#config
SwitchA(config)#router ospf 1
SwitchA(config-router)#network 192.168.0.0 0.0.0.255 area 1
SwitchA(config-router)#network 192.168.1.0 0.0.0.255 area 1
SwitchA(config-router)#network 192.168.100.0 0.0.0.255 area 0
SwitchA(config-router)#
```

步骤 14：在 SwitchB 上配置 OSPF 路由协议。

```
SwitchB#config
SwitchB(config)#router ospf 1
SwitchB(config-router)#network 192.168.2.0 0.0.0.255 area 2
SwitchB(config-router)#network 192.168.3.0 0.0.0.255 area 2
SwitchB(config-router)#network 192.168.100.0 0.0.0.255 area 0
SwitchB(config-router)#
```

步骤 15：查看 SwitchA 的路由表。

```
SwitchA#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
```

```
C       127.0.0.0/8 is directly connected, Loopback
C       192.168.0.0/24 is directly connected, Vlan10
C       192.168.1.0/24 is directly connected, Vlan20
O IA    192.168.2.0/24 [110/20] via 192.168.100.2, Vlan100, 00:00:20
O IA    192.168.3.0/24 [110/20] via 192.168.100.2, Vlan100, 00:00:20
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
SwitchA#
```

步骤 16：查看 SwitchB 的路由表。

```
SwitchB#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback
O IA    192.168.0.0/24 [110/20] via 192.168.100.1, Vlan100, 00:00:06
O IA    192.168.1.0/24 [110/20] via 192.168.100.1, Vlan100, 00:00:06
C       192.168.2.0/24 is directly connected, Vlan30
C       192.168.3.0/24 is directly connected, Vlan40
C       192.168.100.0/24 is directly connected, Vlan100
Total routes are : 6 item(s)
SwitchB#
```

步骤 17：配置了 OSPF 多区域协议后，验证网络的连通性，如图 2-4-22 所示。

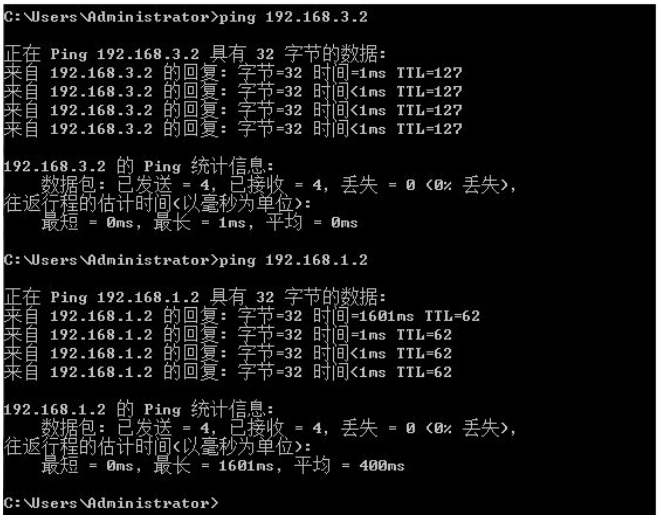


图 2-4-22　连通性测试效果图（二）

学习小结

本学习活动介绍了三层交换机之间如何实现动态 OSPF 路由协议，需要注意的是要先启动 OSPF 协议，再在相应接口配置所属 OSPF 区域，OSPF 骨干区域（area 0）必须保证是连续的。

项目考核

一、选择题

1．VLAN 在现代组网技术中占有重要地位。在由多个 VLAN 组成的一个局域网中，以下说法不正确的是（　　）。

A．当站点从一个 VLAN 转移到另一个 VLAN 时，一般不需要改变物理连接

B．VLAN 中的一个站点可以和另一个 VLAN 中的站点直接通信

C．当站点在一个 VLAN 中广播时，其他 VLAN 中的站点不能收到

D．VLAN 可以通过 MAC 地址、交换机端口等进行定义

2．在默认配置的情况下，交换机的所有端口（　　）。

A．处于直通状态　　B．属于同一 VLAN

C．属于不同 VLAN　　D．地址都相同

3．连接在不同交换机上的，属于同一 VLAN 的数据帧必须通过（　　）传输。

A．服务器　　B．路由器　　C．Backbone 链路　D．Trunk 链路

4．在下面关于 VLAN 的描述中，不正确的是（　　）。

A．VLAN 把交换机划分成多个逻辑上独立的交换机

B．主干链路可以提供多个 VLAN 之间通信的公共通道

C．由于包含了多个交换机，所以 VLAN 扩大了冲突域

D．一个 VLAN 可以跨越多个交换机

5．当数据在两个 VLAN 之间传输时需要（　　）设备。

A．二层交换机　B．网桥　　C．路由器　　D．中继器

6．在一个运行 OSPF 的自治系统之内，（　　）。

A．骨干区域自身也必须是连通的

B．非骨干区域自身也必须是连通的

C．必须存在一个骨干区域（区域号为 0）

D．非骨干区域与骨干区域必须直接相连或逻辑上相连

7．下列关于 OSPF 协议的说法正确的是（　　）。

A．OSPF 支持基于接口的报文验证

B．OSPF 支持到同一目的地址的多条等值路由

C．OSPF 是一个基于链路状态算法的边界网关路由协议

D．OSPF 发现的路由可以根据不同的类型而有不同的优先级

8．下列静态路由配置正确的是（　　）。

A．ip route 129.1.0.0 16 serial 0

B．ip route 10.0.0.2 16 129.1.0.0

C．ip route 129.1.0.0 16 10.0.0.2

D．ip route 129.1.0.0 255.255.0.0 10.0.0.2

9．以下不属于动态路由协议的是（　　）。

A．RIP　　B．ICMP　　C．IS-IS　　D．OSPF

10．三种路由协议 RIP、OSPF、BGP 和静态路由各自得到了一条到达目的网络的路由，默认情况下，最终选定（　　）路由作为最优路由。

A．RIP　　B．OSPF　　C．BGP　　D．静态路由

11．路由环问题会引起（　　）。

A．慢收敛　　B．广播风暴　　C．路由器重启　　D．路由不一致

12．以下路由表项由网络管理员手动配置的是（　　）。

A．静态路由　　B．直接路由　　C．动态路由　　D．以上说法都不正确

13．关于 RIP 协议，下列说法正确的有（　　）。

A．RIP 协议是一种 IGP

B．RIP 协议是一种 EGP

C．RIP 协议是一种距离矢量路由协议

D．RIP 协议是一种链路状态路由协议

14．RIP 协议基于（　　）。

A．UDP　　B．TCP　　C．ICMP　　D．Raw IP

15．RIP 协议的路由项在（　　）时间内没有更新会变为不可达。

A．90s　　B．120s　　C．180s　　D．240s

16．解决路由环路的方法有（　　）。

A．水平分割　　B．抑制时间　　C．毒性逆转　　D．触发更新

二、实操题

配置交换机的优先级，实现网络的负载分担，并配置骨干交换机之间的端口聚合，如图 2-4-23 所示。

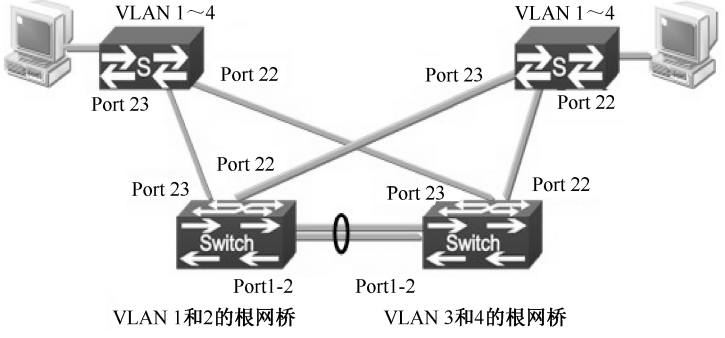
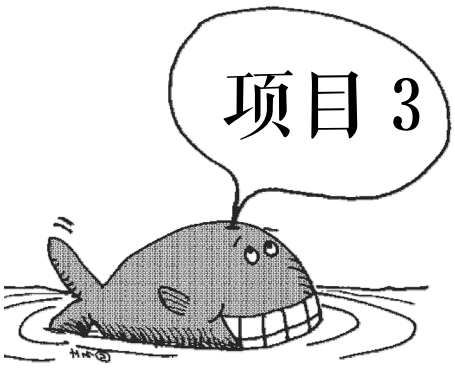


图 2-4-23　网络负载分担拓扑图



路由器的配置

项目学习说明

路由器是连接因特网中各局域网和广域网的不可缺少的网络设备，它会根据整个网络的通信情况自动进行路由选择，以最佳的路径，按先后顺序发送信息给其他网络设备，从而实现信息的路由转发。目前路由器已经广泛应用于各行各业，各种不同档次的产品已经成为实现各种骨干网内部连接、骨干网间互连和骨干网与互联网互连互通业务的主力军。

本项目重点学习路由器的基本配置和路由器的路由配置。

学习能力目标

学习任务 1 路由器的基本配置

学习任务 2 路由器的路由配置

职业能力目标

- 熟练掌握路由器的基本配置命令
- 熟练掌握路由器的单臂路由的配置
- 熟练掌握路由器的 DHCP 服务的配置
- 熟练掌握路由器的静态路由协议配置的实现
- 熟练掌握路由器的动态路由协议配置的实现

学习任务 1　路由器的基本配置

路由器在网络中担任了非常重要的角色，因此路由器的基本配置显得尤为重要。路由器的基本配置主要有：给设备命名、登录信息、接口的 IP 地址、设置特权密码和端口配置等。本学习任务分成以下三个学习活动进行学习。

学习活动 1　路由器的简单配置。
学习活动 2　路由器文件的备份和保存。
学习活动 3　单臂路由的配置。

学习活动 1　路由器的简单配置

学习情境

现因公司业务发展需求，需要购买一台路由器扩展现有网络，根据公司的网络拓扑规划，网络管理员将刚买回来的新路由器配置后，即可投入使用。

情境分析

网络管理员拿到刚买的路由器，第一次对出厂的路由器配置时，可以通过路由器的 Console 口进行。在路由器上有一个 Console 口，可从路由器端口标识中识别到，之后通过出厂自带的配置线进行连接配置。

所需准备：

（1）DCR-2655 路由器 1 台。
（2）PC 1 台。
（3）交叉线缆 1 条。
（4）Console 线 1 条。

路由器基本配置拓扑结构如图 3-1-1 所示。

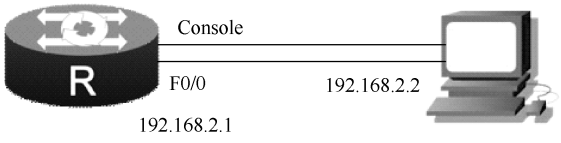


图 3-1-1　路由器基本配置拓扑结构

相关知识

1. 路由器的管理方式

路由器的管理方式可以分为带外管理和带内管理。带内管理，是指网络的管理控制信息与用户网络的承载业务信息通过同一个逻辑信道传送，简而言之，就是占用业务带宽。带外管理，是指网络的管理控制信息与用户网络的承载业务信息在不同的逻辑信道传送，也就是设备提供专门用于管理的带宽。目前很多高端的交换机都带有带外网管接口，使网络管理的带宽和业务带宽完全隔离，互不影响，构成单独的网管网。通过 Console 口管理是最常用的带外管理方式，通常用户会在首次配置交换机或者无法进行带内管理时使用带外管理方式。带外管理方式也是使用频率最高的管理方式。带外管理的时候，我们可以采用 Windows 操作系统自带的超级终端程序来连接交换机，当然，用户也可以采用自己熟悉的终端程序。带外管理方式就是通过路由器的 Console 口管理路由器的方式，不占用路由器的网络接口，但

特点是线缆特殊，需要近距离配置。第一次使用路由器时，必须采用 Console 口对路由器进行配置，使其支持 Telnet 远程管理。带内管理的方式有 Telnet 方式和 Web 方式。

2. 路由器的命令行操作模式

路由器的命令行操作模式主要有：用户模式、特权模式、全局配置模式。

用户模式：进入路由器后得到的第一个操作模式，此模式下用户只具有最底层的权限，可以查看路由器的软、硬件版本信息，但不能对路由器进行配置。

特权模式：用户模式的下一级模式，此模式下用户可以对路由器的配置文件进行管理，查看路由器的配置信息，进行网络的测试和调试等。

全局配置模式：特权模式的下一级模式，此模式下可以配置路由器的全局参数，如主机名、登录信息等，在此模式下可以进入下一级的配置模式，对路由器具体的功能进行配置。

步骤实现

步骤 1：用 Console 线将路由器的 Console 口与 PC 的串口相连。

步骤 2：在 PC 上运行终端仿真程序。执行“开始”→“程序”→“附件”→“通信”→“超级终端”命令，弹出“COM8 属性”对话框，同时设置终端的硬件参数，如图 3-1-2 所示。

图 3-1-2　终端仿真配置图

步骤 3：路由器加电，超级终端显示路由器的自检信息，自检结束后出现如下命令提示。

```
“press RETURN to get started”。
System Bootstrap, Version 0.1.8
Serial num:8IRT01V11B01000054 ,ID num:000847
Copyright (c) 1996-2000 by China Digitalchina CO.LTD
DCR-1700 Processor MPC860T @ 50Mhz
The current time: 2067-9-12 6:31:30
Loading DCR-1702.bin......
Start Decompress DCR-1702.bin
################################################################################
################################################################################
################################################################################
```

```
    ######################################################################
    ######## Decompress 3587414 byte,Please wait system up..
    Digitalchina Internetwork Operating System Software
    DCR-1700 Series Software , Version 1.3.2E, RELEASE SOFTWARE
    System start up OK
    Router console 0 is now available
    Press RETURN to get started
```

步骤 4 :按【Enter】键进入用户配置模式。DCR 路由器出厂时没有定义密码, 用户按【Enter】键即可直接进入普通用户模式，可以使用权限允许范围内的命令，需要帮助可以随时输入“？”，输入“ enable ”，按【Enter】键即可进入超级用户模式，在超级配置模式下，用户拥有最大的权限，可以任意配置，需要帮助可以随时输入“？”。

```
    Router-A>enable                              ！进入特权模式
    Router-A#2004-1-1 00:04:39 User DEFAULT enter privilege mode from console 0,
level = 15
    Router-A#?                                   ！查看可用的命令
    cd -- Change directory
    chinese -- Help message in Chinese
    chmem -- Change memory of system
    chram -- Change memory
    clear -- Clear something
    config -- Enter configurative mode
    connect -- Open a outgoing connection
    copy -- Copy configuration or image data
    date -- Set system date
    debug -- Debugging functions
    delete -- Delete a file
    dir -- List files in flash memory
    disconnect -- Disconnect an existing outgoing network
    connection
    download -- Download with ZMODEM
    enable -- Turn on privileged commands
    english -- Help message in English
    enter -- Turn on privileged commands
    exec-script -- Execute a script on a port or line
    exit -- Exit / quit
    format -- Format file system
    help -- Description of the interactive help system
    history -- Look up history
    Router-A#ch?                                      ！使用？帮助
    chinese -- Help message in Chinese
    chmem -- Change memory of system
    chram -- Change memory
    Router-A#chinese                                  ！设置中文帮助
    Router-A#?                                        ！再次查看可用命令
```

```
cd                                          -- 改变当前目录
Chinese                                     -- 中文帮助信息
chmem                                       -- 修改系统内存数据
chram                                       -- 修改内存数据
clear                                       -- 清除
config                                      -- 进入配置状态
connect                                     -- 打开一个向外的连接
copy                                        -- 复制配置方案或内存映像
date                                        -- 设置系统时间
debug                                       -- 分析功能
delete                                      -- 删除一个文件
dir                                         -- 显示闪存中的文件
disconnect                                  -- 断开活跃的网络连接
download                                    -- 通过ZMODEM协议下载文件
enable                                      -- 进入特权方式
english                                     -- 英文帮助信息
enter                                       -- 进入特权方式
exec-script                                 -- 在指定端口运行指定的脚本
exit                                        -- 退回或退出
format                                      -- 格式化文件系统
help                                        -- 交互式帮助系统描述
history                                     -- 查看历史
keepalive                                   -- 保活探测
--More—
```

步骤 5：设置路由器以太网接口地址并验证连通性。

```
Router>enable                                        ！进入特权模式
Router #config                                       ！进入全局配置模式
Router_ config#interface f0/0                        ！进入接口模式
Router_config_f0/0#ip address 192.168.2.1 255.255.255.0  ！设置IP地址
Router_config_f0/0#no shutdown
Router config f0/0#^Z
Router#show interface f0/0                           ！验证
FastEthernet0/0 is up, line protocol is up     ！接口和协议都必须up
address is 00e0.0f18.1a70
Interface address is 192.168.2.1/24
MTU 1500 bytes, BW 100000 kbit, DLY 10 usec
Encapsulation ARPA, loopback not set
Keepalive not set
ARP type: ARPA, ARP timeout 04:00:00
60 second input rate 0 bits/sec, 0 packets/sec!
60 second output rate 6 bits/sec, 0 packets/sec!
Full-duplex, 100Mb/s, 100BaseTX, 1 Interrupt
0 packets input, 0 bytes, 200 rx freebuf
Received 0 unicasts, 0 lowmark, 0 ri, 0 throttles
```

```
0 input errors, 0 CRC, 0 framing, 0 overrun, 0 long
1 packets output, 46 bytes, 50 tx freebd, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred, 0 err600
0 lost carrier, 0 no carrier 0 grace stop 0 bus error
0 output buffer failures, 0 output buffers swapped out
```

步骤 6：设置 PC 的 IP 地址，如图 3-1-3 所示。

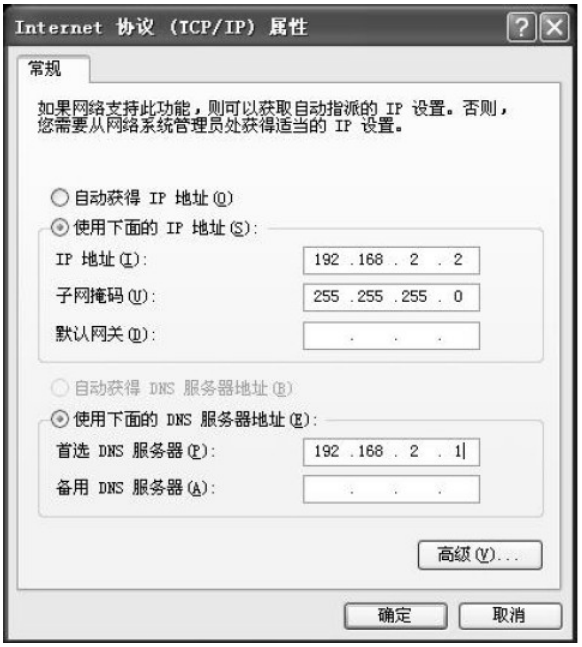


图 3-1-3　设置 PC 的 IP 地址

使用 ping 命令测试连通性，如图 3-1-4 所示。

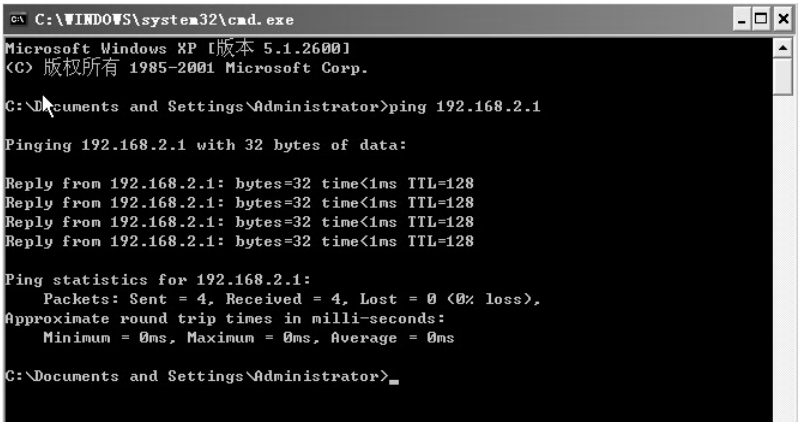

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator>

图 3-1-4　连通性测试效果图

小贴士

（1）在超级终端中的配置是对路由器的操作，这时的 PC 只是输入输出设备。

（2）计算机和路由器直连需要使用交叉线，否则计算机将无法 ping 通路由器。

（3）要按照（9600，8，无，1，无）设置终端的硬件参数，否则计算机将无法 ping 通路由器。

（4）要选择正确的计算机 COM 口。

知识拓展

如果配置好路由器的接口 IP 地址且能进行网络通信，则可以通过局域网或广域网，使用 Telnet 客户端登录到路由器上，对路由器进行本地或者远程的配置。这样可以降低管理员的工作量。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。

（4）Console 线 1 条。

（5）交叉线 1 条。

Telnet 访问路由器网络拓扑结构如图 3-1-5 所示。

网络设备和 PC 的 IP 地址网络参数设置见表 3-1-1。

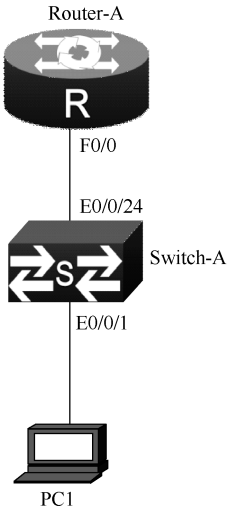


图 3-1-5　Telnet 访问路由器网络拓扑结构

表 3-1-1　网络设备和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Router-A	F0/0	192.168.1.1	255.255.255.0	无
Switch-A	VLAN1	192.168.1.10	255.255.255.0	192.168.1.1
	E0/0/1	无	无	无
	E0/0/24	无	无	无
PC1		192.168.1.2	255.255.255.0	192.168.1.1

步骤 1：按照图 3-1-5 连接网络拓扑结构。

步骤 2：按照表 3-1-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复交换机的出厂配置。

步骤 4：恢复路由器的出厂配置。

```
    Router>enable                                          ! 进入特权模式
    Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
    Router#delete                                          ! 删除配置文件
    this file will be erased,are you sure?(y/n)y
    Router#reboot                                          ! 重新启动
    Do you want to reboot the router(y/n)?y
    Please wait…..
```

步骤 5：设置交换机 A 的主机名和管理 IP 地址。

```
DCS-3950-26C>enable
DCS-3950-26C#config
DCS-3950-26C(config)#host Switch-A
Switch-A(config)#int vlan 1
Switch-A(config-if-vlan1)#
Switch-A(config-if-vlan1)#ip add 192.168.1.10 255.255.255.0
Switch-A(config-if-vlan1)#exit
Switch-A(config)#ip default-gateway 192.168.1.1
Switch-A(config)#
```

步骤 6：设置路由器 A 的主机名称和接口 IP 地址。

```
Router>enable                                          !进入特权模式
Router #config                                         !进入全局配置模式
Router _config#hostname Router-A                       !修改机器名
Router-A_config#int fa0/0                              !进入接口
Router-A_config_f0/0#ip add 192.168.1.1 255.255.255.0 !配置IP地址
Router-A_config_f0/0#no shut                           !开启端口
```

步骤 7：查看路由器 A 的端口 IP 地址配置情况。

```
Router-A#show ip int brief
Interface               IP-Address     Method Protocol-Status
Async0/0                unassigned     manual down
Serial0/1               unassigned     manual down
Serial0/2               unassigned     manual down
FastEthernet0/0         192.168.1.1     manual up
FastEthernet0/3         unassigned     manual down
Router-A#
```

步骤 8：设置特权模式密码。

```
Router-A_config#enable password 0 digital              !0表示明文
Router-A config# aaa authentication enable default enable
Router-A config#^Z
Router-A#2004-1-1 16:38:49 Configured from console 0 by DEFAULT
Router-A#exit
Router-A>enable                                        !再次进入特权模式
Password:                                              !需要输入密码
Access deny !
Router-A>enable
Password:                                              !注意输入时不显示密码
Router-A#2004-1-1 16:39:14 User DEFAULT enter privilege mode from console 0,
level = 15
Router-A#
```

步骤 9：保存设置。

```
Router-A#write                                            !保存设置
Saving current configuration...
OK!
```

步骤 10：配置 Telnet。

```
Router-A config#username zwk password 0 123456
                                    ！定义Telnet用户名为zwk，密码为123456
Router-A_config#aaa authentication login telnet local
                    ！开启路由器登录认证，定义该登录认证过程名为Telnet
Router-A_config#line vty 0 4        ！进入虚拟Telnet接口
Router_config_line#login authentication telnet
                                    ！将登录认证过程Telnet应用到虚拟的Telnet接口
```

步骤 11：Telnet 测试。

（1）执行“开始”→“运行”命令，弹出“打开”对话框，在“打开”文本框中输入“telnet 192.168.1.1”，如图 3-1-6 所示。

（2）在“Username”栏中输入“zwk”，在“Password”栏中输入“123456”，如图 3-1-7 所示，出现“Router>-A”，表示远程登录成功。

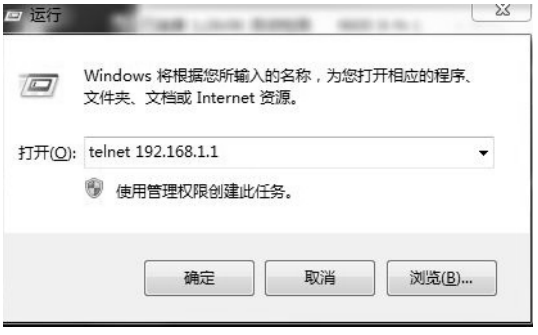


图 3-1-6　运行 Telnet 路由器

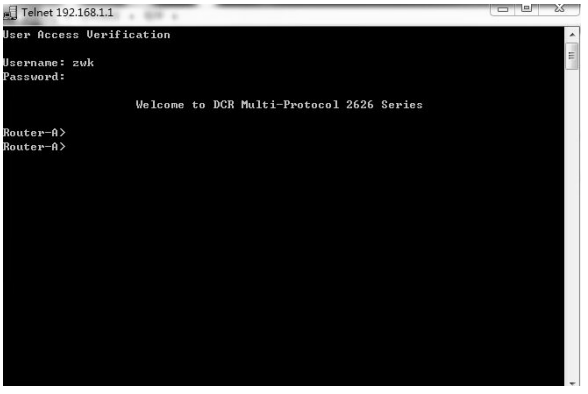


图 3-1-7　Telnet 路由器效果图

小贴士

（1）CR-V35FC 所连的接口为 DCE，需要配置时钟频率，CR-V35MT 所连的接口为 DTE。

（2）查看接口状态，如果接口是 down，通常是线缆出现了故障；如果协议是 down，通常是时钟频率没有配置，或者两端封装协议不一致。

学习小结

本学习活动重点介绍了路由器的基本设置，基础知识掌握牢固很重要，Console 口和 Telnet 的管理方式更要求读者能够灵活应用，企业中 Telnet 的管理方式在后期网络设备的维护中使用更多。

学习活动 2　路由器文件的保存和备份

学习情境

某公司的网络管理员对公司的路由器进行了完整的配置，可以使公司的网络正常工作，但现在网络管理员想对路由器的文件进行保存和备份。

情境分析

网络管理员将公司路由器配置完成后，必须要对其进行保存和备份，这是网络管理员的重要工作之一。当日后路由器文件损坏时，可以快速地将文件恢复过来。

所需准备：

（1）DCR-2655 路由器 1 台。

（2）PC 1 台。

（3）TFTP 软件。

（4）Console 线 1 条。

（5）交叉线 1 条。

维护路由器配置文件拓扑结构如图 3-1-8 所示。

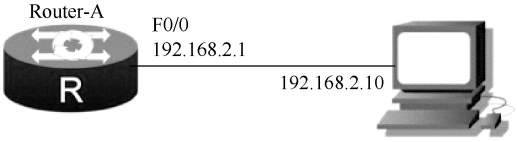


图 3-1-8　维护路由器配置文件拓扑结构

相关知识

路由器文件的保存在特权模式下进行，使用 write 命令即可。

可以将 startup-config 的文件经过 TFTP 软件备份到计算机中，以便下次路由器出现故障时直接恢复。

路由器的系统文件存储在 Flash 中，如果 Flash 中的配置文件遭到破坏，路由器无法正常工作，可以通过 TFTP 软件进行恢复，即从备份的路由器 Flash 中将文件写到路由器中。如果系统文件没有损坏，而路由器的文件丢失了，则直接恢复文件即可。

TFTP 是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务，其端口号为 69。

步骤实现

1. 路由器的保存

```
Router-A#write
Saving current configuration...
OK!
```

2. 路由器配置文件的备份

步骤 1：按照图 3-1-8 连接网络拓扑结构。

步骤 2：设置 PC 网卡地址为 192.168.2.10，并安装 TFTP Server，如图 3-1-9 所示。

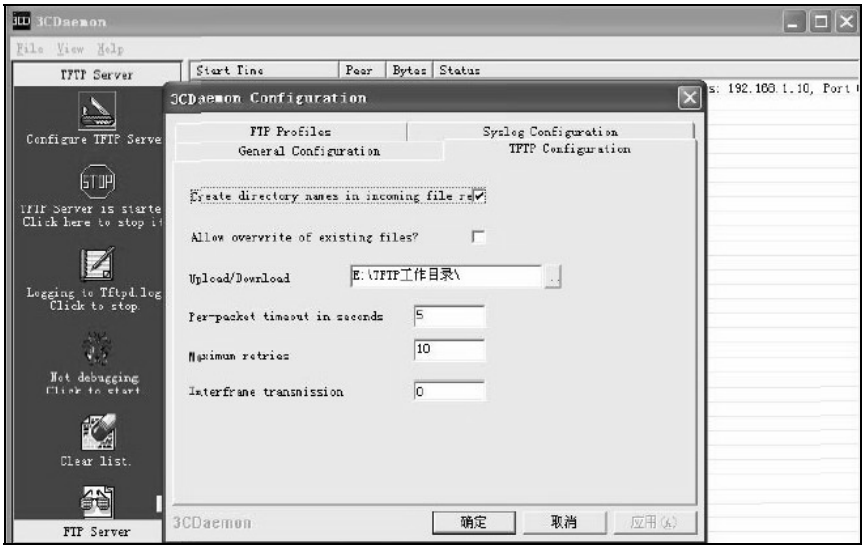


图 3-1-9　安装 TFTP Server

步骤 3：设置 Router-A 的 F0/0 接口地址为 192.168.2.1，并测试连通性。

```
Router-A#config
Router-A_config#interface f0/0
Router-A config f0/0#ip address 192.168.2.1 255.255.255.0
Router-A config f0/0#no shutdown
Router-A_config_f0/0#^Z
Router-A#show interface f0/0
FastEthernet0/0 is up, line protocol is up
address is 00e0.0f18.1a70
Interface address is 192.168.2.1/24
MTU 1500 bytes, BW 100000 kbit, DLY 10 usec
Encapsulation ARPA, loopback not set
Keepalive not set
<省略。。。>
Router-A#ping 192.168.2.10 ！Ping PC的IP地址
PING 192.168.2.10 (192.168.2.1): 56 data bytes
!!!!!
--- 192.168.2.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 20/22/30 ms
```

步骤 4：查看路由器文件，并将配置文件下载到 TFTP 服务器上。

```
Router-A#dir
Directory of /:
0    DCR26V1.3.3H.bin     <FILE>     5474750    Tue Jan  1 00:02:51 2002
1    Function.map         <FILE>      784567    Tue Jan  1 00:03:10 2002
2    startup-config       <FILE>         648    Tue Jan  1 02:07:23 2002
free space 2064384
Router-A#copy flash:startup-config tftp:          ! 上传配置文件作为备份
Remote-server ip address[]?192.168.2.10           ! TFTP服务器的IP地址
Destination file name[startup-config]?            ! 默认的文件名
#
TFTP:successfully send 2 blocks ,516 bytes
```

步骤 5：使用写字板打开下载后的配置文件，修改机器名称，上传到路由器中，重新启动后通过 show 命令观察到机器名已经被修改。

小贴士

（1）路由器和 PC 直接相连的时候，应使用交叉线。

（2）要保证路由器和 TFTP 服务器的连通性。

（3）关闭 PC 上的防火墙。

学习小结

本学习活动介绍了路由器的保存和备份，这对管理员来说是至关重要的，在备份时要注意保存的文件名和保存位置。

学习活动 3　单臂路由的配置

学习情境

公司的网络管理员对部门划分 VLAN 后，发现两个部门之间无法通信了，但有时两个部门的员工需要进行通信，网络管理员现要通过简单的方法来实现这一功能。

情境分析

通过在交换机上划分适当数目的 VLAN，不仅能有效隔离广播风暴，还能提高安全性及网络带宽的利用效率。划分 VLAN 之后，VLAN 与 VLAN 之间是不能通信的，使用路由器

的单臂路由功能可以解决这个问题。

所需准备：

（1）DCS-3950 二层交换机 1 台。

（2）DCR-2655 路由器 1 台。

（3）交换机和路由器 Console 线各 1 条。

（4）直通双绞线 3 条。

单臂路由配置拓扑结构如图 3-1-10 所示。

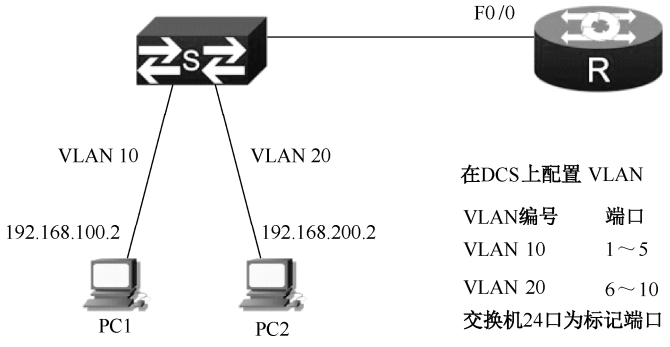


图 3-1-10 单臂路由配置拓扑结构

相关知识

单臂路由，即在路由器上设置多个逻辑子接口，每个子接口对应一个 VLAN。每个子接口的数据在物理链路上传递都要标记封装。对于路由器的端口，在支持子接口的同时，还必须支持 Trunk 功能。

使用单臂路由器模式配置 VLAN 间路由时，路由器的物理接口必须与相邻交换机的 Trunk 链路相连。在路由器上，子接口是为网络上每个唯一 VLAN 而创建的。每个子接口会分配专属于其子网/VLAN 的 IP 地址，同时也便于为该 VLAN 标记帧。这样，路由器可以在流量通过 Trunk 链路返回交换机时区分不同子接口的流量。

路由器一般是基于软件处理方式来实现路由的，存在一定的延时，难以达到线速交换。所以，随着 VLAN 通信流量的增多，路由器将成为通信的瓶颈。因此，单臂路由适用于通信流量较少的情况。

配置子接口的封装类型和所属 VLAN 的命令如下：

```
Router_config#interface f0/0
Router config f0/0#no shutdown
Router_config_f0/0#interface f0/0.1          ！进入f0/0.1子接口
Router_config_f0/0.1#encapsulation dot1q 10 ！封装trunk协议dot1q，10为vlan号
```

步骤实现

步骤 1：按照图 3-1-10 连接网络拓扑结构。

步骤 2：配置 PC1 的地址及网关，如图 3-1-11 所示。

步骤 3：配置 PC2 的地址及网关，如图 3-1-12 所示。

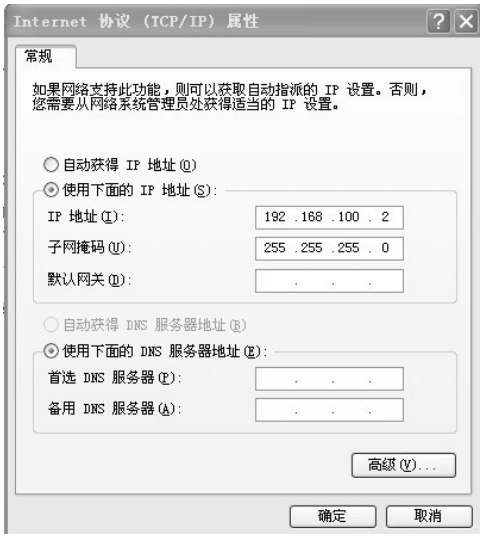


图 3-1-11　配置 PC1 的地址及网关

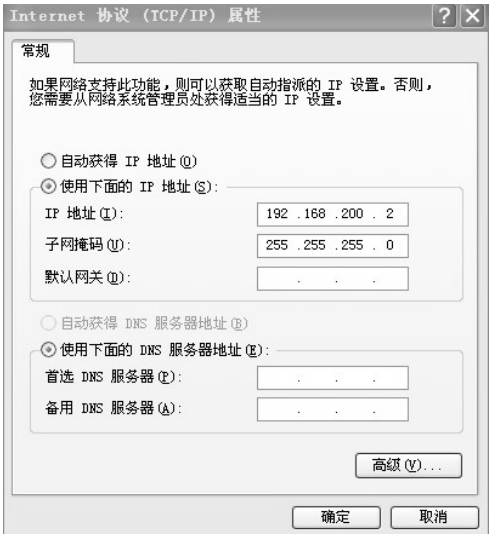


图 3-1-12　配置 PC2 的地址及网关

步骤 4：恢复路由器的出厂配置。

```
Router>enable                                          ! 进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          ! 删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ! 重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 5：恢复交换机出厂设置。

```
switch>enable                                          ! 进入特权配置模式
switch#set default                                     ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 6：在交换机 DCS 上设置主机名。

```
switch>enable
switch#config terminal
switch(Config)#hostname DCS
DCS(Config)#
```

步骤 7：在交换机 DCS 上创建 VLAN10，端口组成员为 1～5，创建 VLAN20，端口组成员为 6～10。

```
DCS(Config)#vlan 10
DCS(Config-Vlan100)#switchport interface e0/0/1-5
DCS(Config-Vlan100)#vlan 20
DCS(Config-Vlan200)#switchport interface e0/0/6-10
```

步骤 8：在交换机 DCS 上配置 Trunk。

```
DCS(Config)#interface ethernet 0/0/24
DCS(Config-Ethernet0/0/24)#switchport mode trunk
```

步骤 9：路由器配置。

```
Router config#interface f0/0
Router_config_f0/0#no ip add
Router config f0/0#no shutdown
Router config#interface f0/0.1
Router_config_f0/0.1#encapsulation dot1q 10
Router config f0/0.1#ip address 192.168.100.1 255.255.255.0
Router config#interface f0/0.2
Router_config_f0/0.2#encapsulation dot1q 20
Router_config_f0/0.2#ip address 192.168.200.1 255.255.255.0
```

步骤 10：测试连通性。PC1 ping PC2，网络已连通，如图 3-1-13 所示。

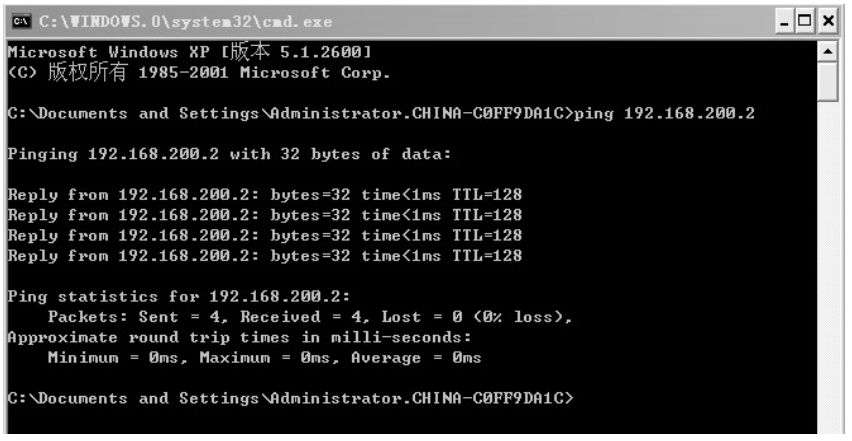

C:\WINDOWS.0\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator.CHINA-C0FF9DA1C>ping 192.168.200.2
Pinging 192.168.200.2 with 32 bytes of data:
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Reply from 192.168.200.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.200.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator.CHINA-C0FF9DA1C>

图 3-1-13　连通性测试效果图

小贴士

（1）此时在以太网接口 f0/0 中不要配置 IP 地址，因为这种情况下的物理接口在配置封装之后仅仅作为一个二层的链路通道存在，而不是具备三层地址的接口。

（2）路由器中一定要创建两个 VLAN 才能进行后续配置。

（3）测试时不可以使用 VLAN1 的成员进行测试，单臂路由不可以使 Trunk 接口与主 VLAN 成员连通。

学习小结

本学习活动重点讲述了使用路由器实现不同 VLAN 间的相互通信，在实现过程中，重点理解子接口的概念，单臂路由适合流量比较小的情况，如果流量比较大，则容易产生瓶颈，造成网络瘫痪。

学习任务 2　路由器的路由配置

在实际应用中路由器通常连接着许多不同的网络，要实现多个不同网络间的通信，则要在路由器上配置路由协议。路由器提供的路由协议包括静态路由协议、RIP 动态路由、OSPF 动态路由协议等。

本学习任务重点学习路由器的路由协议的配置，分为以下三个学习活动进行。

学习活动 1　路由器的静态路由配置。

学习活动 2　路由器的 RIP 动态路由配置。

学习活动 3　路由器的 OSPF 动态路由配置。

学习活动 1　路由器的静态路由配置

静态路由是指由网络管理员手工配置的路由信息。当网络的拓扑结构或链路状态发生变化时，网络管理员要手工修改路由表中的静态路由信息。静态路由信息在默认情况下不会传递给其他的路由器。静态路由一般适用于比较简单的网络环境。

学习情境

某公司刚成立，规模很小，只有两台路由器。该公司的网络管理员经过考虑，决定在公司的路由器与运营商路由器之间使用静态路由，实现网络的互连。

情境分析

由于该网络规模较小且不经常变动，所以使用静态路由比较合适。两台路由器之间通过以太网口相连，每台路由器连接一台计算机。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）交叉线 3 条。

静态路由拓扑结构如图 3-2-1 所示。

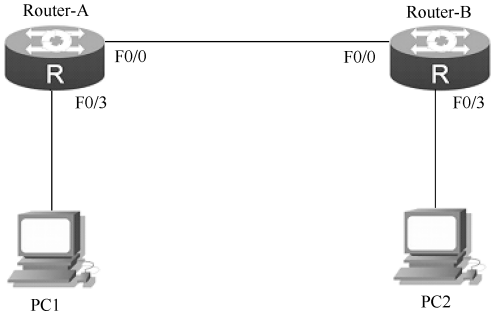


图 3-2-1　静态路由拓扑结构

路由器和 PC 的 IP 地址网络参数设置见表 3-2-1。

表 3-2-1　路由器和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Router-A	F0/0	192.168.1.1	255.255.255.0	无
	F0/3	192.168.10.1	255.255.255.0	无
Router-B	F0/0	192.168.1.2	255.255.255.0	无
	F0/3	192.168.20.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

相关知识

1. 路由表的产生方式

路由器在转发数据时，首先要在路由表中查找相应的路由。路由表的产生方式有三种。

（1）直连网络：路由器自动添加和自己直接连接的网络路由。

（2）静态路由：由网络管理员手工配置的路由信息。当网络的拓扑结构或链路发生变化时，需要网络管理员手动修改路由表中的相关路由信息。

（3）动态路由：由路由协议动态产生的路由。

2. 静态路由的优缺点

静态路由优点：使用静态路由的好处是网络安全保密性高。动态路由因为需要路由器之间频繁地交换各自的路由表，而对路由表的分析可以揭示网络的拓扑结构和网络地址等信息。因此，出于网络安全方面的考虑可以采用静态路由。

静态路由缺点：大型和复杂的网络环境通常不宜采用静态路由。一方面，网络管理员难以全面地了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这一工作的难度和复杂程度非常高。

在小型的网络中，使用静态路由是较好的选择，网络管理员想控制数据转发路径时，也会使用静态路由。

静态路由的配置命令是如下：

```
ip route 目的网络的IP 地址 子网掩码 下一跳IP地址/本地接口
```

步骤实现

步骤 1：按照图 3-2-1 连接网络拓扑结构。

步骤 2：按照表 3-2-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          ！删除配置文件
```

```
this file will be erased,are you sure?(y/n)y
Router#reboot                                          !重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router>
Router>ena
Router#Jan  1 00:05:06 Unknown user enter privilege mode from console 0, level
= 15
Router#config
Router config#hostname Router-A
Router-A_config_f0/0#ip address 192.168.1.1 255.255.255.0
Router-A config f0/0#no shutdown
Router-A config f0/0#int fa0/3
Router-A_config_f0/3#ip add 192.168.10.1 255.255.255.0
Router-A config f0/3#no shutdown
Router-A config f0/3#^Z
Router-A#
```

步骤 5：配置 Router-B 的名称及其接口 IP 地址。

```
Router>
Router>enable
Router#Jan  1 00:05:06 Unknown user enter privilege mode from console 0, level
= 15
Router#config
Router_config#hostname Router-B
Router-B config#int fa0/0
Router-B config f0/0#ip add 192.168.1.2 255.255.255.0
Router-B_config_f0/0#no shut
Router-B config f0/0#int fa0/3
Router-B config f0/3#ip add 192.168.200.1 255.255.255.0
Router-B_config_f0/3#ip add 192.168.20.1 255.255.255.0
Router-B config f0/3#no shut
Router-B config f0/3#^Z
Router-B#
```

步骤 6：查看 Router-A 接口的配置情况。

```
Router-A#show ip int brief
Interface               IP-Address      Method    Protocol-Status
Async0/0                unassigned      manual        down
Serial0/1               unassigned      manual        down
Serial0/2               unassigned      manual        down
FastEthernet0/0         192.168.1.1     manual        up
FastEthernet0/3         192.168.10.1    manual        up
Router-A#
```

步骤 7：查看 Router-B 接口的配置情况。

```
Router-B#show ip int brief
Interface               IP-Address      Method    Protocol-Status
Async0/0                unassigned      manual         down
Serial0/1               unassigned      manual         down
Serial0/2               unassigned      manual         down
FastEthernet0/0         192.168.1.2     manual         up
FastEthernet0/3         192.168.20.1    manual         up
Router-B#
```

步骤 8：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.10.0/24     is directly connected, FastEthernet0/3
Router-A#
```

步骤 9：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.20.0/24     is directly connected, FastEthernet0/3
Router-B#
```

步骤 10：配置路由协议前，使用 ping 命令测试网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络未连通，如图 3-2-2 所示。

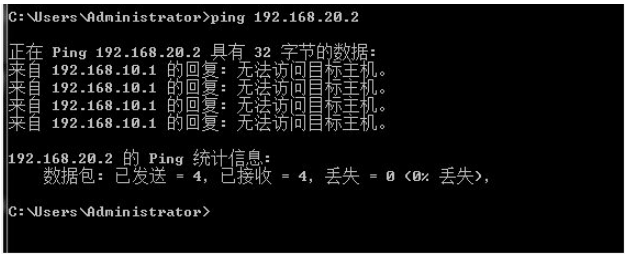


图 3-2-2　连通性测试效果图（一）

（2）在 PC2 上 ping 192.168.10.2，如图 3-2-3 所示，网络未通。

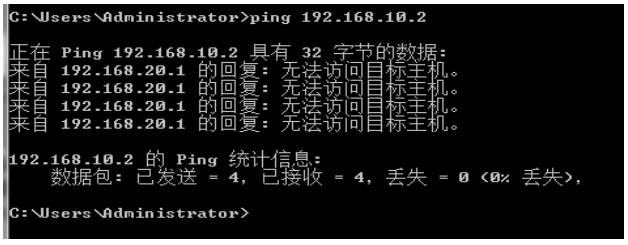


图 3-2-3 连通性测试效果图（二）

步骤 11：在 Router-A 上配置静态路由。

```
Router-A#config
Router-A_config#ip route 192.168.20.0 255.255.255.0 192.168.1.2
Router-A_config#
```

步骤 12：在 Router-B 上配置静态路由。

```
Router-B#config
Router-B_config#ip route 192.168.10.0 255.255.255.0 192.168.1.1
Router-B_config#
```

步骤 13：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.10.0/24     is directly connected, FastEthernet0/3
S     192.168.20.0/24     [1,0] via 192.168.1.2(on FastEthernet0/0)
Router-A#                                        ！注意静态路由的管理距离是1
```

步骤 14：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.20.0/24     is directly connected, FastEthernet0/3
S     192.168.10.0/24     [1,0] via 192.168.1.1(on FastEthernet0/0)
```

```
Router-B#                                        ！注意静态路由的管理距离是1
```

步骤 15：配置路由协议后，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络已连通，如图 3-2-4 所示。

C:\Users\Administrator>ping 192.168.20.2
正在 Ping 192.168.20.2 具有 32 字节的数据:
来自 192.168.20.2 的回复: 字节=32 时间=4ms TTL=126
来自 192.168.20.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.20.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.20.2 的回复: 字节=32 时间=1ms TTL=126
192.168.20.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 1ms, 最长 = 4ms, 平均 = 1ms
C:\Users\Administrator>

图 3-2-4　连通性测试效果图（三）

（2）在 PC2 上 ping 192.168.10.2，网络已连通，如图 3-2-5 所示。

C:\Users\Administrator>ping 192.168.10.2
正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
192.168.10.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 1ms, 最长 = 1ms, 平均 = 1ms
C:\Users\Administrator>

图 3-2-5　连通性测试效果图（四）

小贴士

（1）在配置静态路由时，必须双向配置才能互通。

（2）非直连的网段都要配置路由。

（3）两台路由器如果使用串口连接，则必须将其中一端设置为 DCE 端。

知识拓展

默认路由是一种特殊的静态路由，指的是当路由表中与数据报的目的地址之间没有匹配的表项时，路由器能够做出的选择。如果没有默认路由，那么目的地址在路由表中没有匹配表项的数据报将被丢弃。默认路由在某些时候非常有效，当存在末梢网络时，默认路由会大大简化路由器的配置，减轻网络管理员的工作负担，提高网络性能。

默认路由和静态路由的命令格式一样。只是把目的 IP 地址和子网掩码改成了 0.0.0.0 和 0.0.0.0。默认路由的配置命令如下：

```
ip route 0.0.0.0 0.0.0.0 下一跳IP地址
```

默认路由的拓扑结构如图 3-2-6 所示。

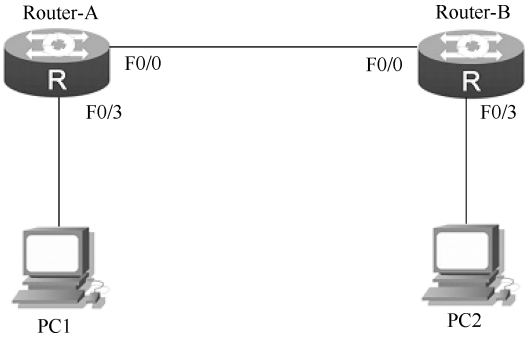


图 3-2-6　默认路由拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 3-2-2。

表 3-2-2　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Router-A	F0/0	192.168.1.1	255.255.255.0	无
	F0/3	192.168.10.1	255.255.255.0	无
Router-B	F0/0	192.168.1.2	255.255.255.0	无
	F0/3	192.168.20.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 3-2-6 连接网络拓扑结构。

步骤 2：按照表 3-2-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
    Router>enable                                              ! 进入特权模式
    Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
    Router#delete                                              ! 删除配置文件
    this file will be erased,are you sure?(y/n)y
    Router#reboot                                              ! 重新启动
    Do you want to reboot the router(y/n)?y
    Please wait…
```

步骤 4：在 Router-A 接口上配置 IP 地址。

```
    Router>
    Router>enable
    Router#config
    Router config#hostname Router-A
    Router-A_config_f0/0#ip address 192.168.1.1 255.255.255.0
    Router-A config f0/0#no shutdown
    Router-A_config_f0/0#int fa0/3
```

```
Router-A_config_f0/3#ip add 192.168.10.1 255.255.255.0
Router-A config f0/3#no shutdown
Router-A config f0/3#^Z
Router-A#
```

步骤 5：在 Router-B 接口上配置 IP 地址。

```
Router>
Router>enable
Router#config
Router config#hostname Router-B
Router-B_config#int fa0/0
Router-B config f0/0#ip add 192.168.1.2 255.255.255.0
Router-B_config_f0/0#no shut
Router-B config f0/0#int fa0/3
Router-B config f0/3#ip add 192.168.200.1 255.255.255.0
Router-B_config_f0/3#ip add 192.168.20.1 255.255.255.0
Router-B config f0/3#no shut
Router-B config f0/3#^Z
Router-B#
```

步骤 6：查看 Router-A 接口的地址配置情况。

```
Router-A#show ip int brief
Interface               IP-Address      Method   Protocol-Status
Async0/0                unassigned      manual       down
Serial0/1               unassigned      manual       down
Serial0/2               unassigned      manual       down
FastEthernet0/0         192.168.1.1     manual       up
FastEthernet0/3         192.168.10.1    manual       up
Router-A#
```

步骤 7：查看 Router-B 接口的地址配置情况。

```
Router-B#show ip int brief
Interface               IP-Address      Method   Protocol-Status
Async0/0                unassigned      manual        down
Serial0/1               unassigned      manual        down
Serial0/2               unassigned      manual        down
FastEthernet0/0         192.168.1.2     manual        up
FastEthernet0/3         192.168.20.1    manual        up
Router-B#
```

步骤 8：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.10.0/24     is directly connected, FastEthernet0/3
Router-A#
```

步骤 9：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.20.0/24     is directly connected, FastEthernet0/3
Router-B#
```

步骤 10：配置路由协议前，使用 ping 命令测试网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络未连通，如图 3-2-7 所示。

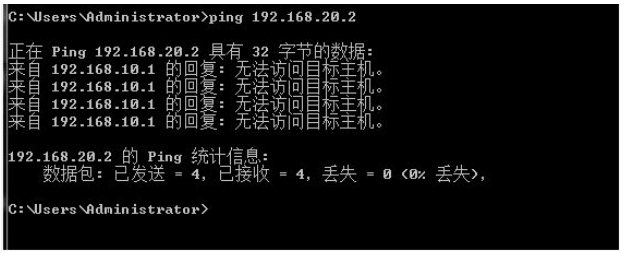


图 3-2-7　连通性测试效果图（一）

（2）在 PC2 上 ping 192.168.10.2，网络未连通，如图 3-2-8 所示。

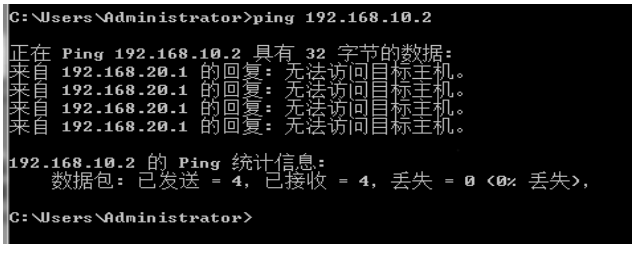


图 3-2-8　连通性测试效果图（二）

步骤 11：在 Router-A 上配置默认路由。

```
Router-A#config
Router-A config#ip route 0.0.0.0 0.0.0.0 192.168.1.2
Router-A_config#
```

步骤 12：在 Router-B 上配置默认路由。

```
Router-B#config
```

```
Router-B_config#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Router-B_config#
```

步骤 13：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S      0.0.0.0/0           [1,0] via 192.168.1.2(on FastEthernet0/0)
C      192.168.1.0/24       is directly connected, FastEthernet0/0
C      192.168.10.0/24      is directly connected, FastEthernet0/3
Router-A#
```

步骤 14：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S      0.0.0.0/0          [1,0] via 192.168.1.1(on FastEthernet0/0)
C      192.168.1.0/24      is directly connected, FastEthernet0/0
C      192.168.20.0/24     is directly connected, FastEthernet0/3
Router-B#
```

步骤 15：验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络已连通，如图 3-2-9 所示。

图 3-2-9　连通性测试效果图（三）

（2）在 PC2 上 ping 192.168.10.2，网络已连通，如图 3-2-10 所示。

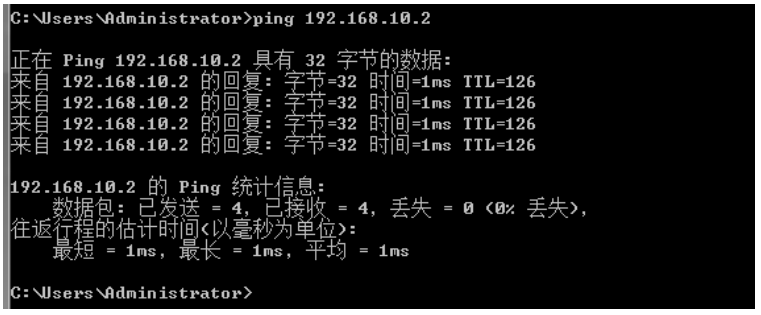

C:\Users\Administrator>ping 192.168.10.2
正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.10.2 的回复: 字节=32 时间=1ms TTL=126
192.168.10.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 1ms, 最长 = 1ms, 平均 = 1ms
C:\Users\Administrator>

图 3-2-10　连通性测试效果图（四）

学习小结

本学习活动介绍了路由器之间如何实现静态路由，需要注意的是添加静态路由时非直连网段也要进行配置。静态路由开销小，但不灵活，只适用于相对稳定的网络。在小型网络环境中，选择静态路由是可以的，但对于中大型网络而言，静态路由的工作量就很大了。

学习活动 2　路由器的 RIP 动态路由配置

在路由器较多的网络环境中，手工配置静态路由会给管理员带来很大的工作负担，那么使用动态路由协议可以很好地解决此问题。RIP 是应用较早、使用较普遍的动态路由协议，也是内部网关协议，由于 RIP 跳数作为衡量路径的开销，且规定最大跳数为 15，因此 RIP 在实际应用中还是有一定限制的，通常适用于中小型的企业网络。

学习情境

随着公司规模的不断扩大，路由器的数量已经达到了 5 台。该公司的网络管理员发现原有的静态路由已经不适合现在的公司。因此，决定在公司的路由器之间使用动态的 RIP 路由协议，实现网络的互连。

情境分析

由于公司的网络规模开始扩大，网络管理员发现使用静态路由确实不合适了，所以决定使用动态的 RIP 路由协议。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）PC 2 台。

（3）交叉线 3 条。

利用 RIP 实现网络连通的拓扑结构如图 3-2-11 所示。

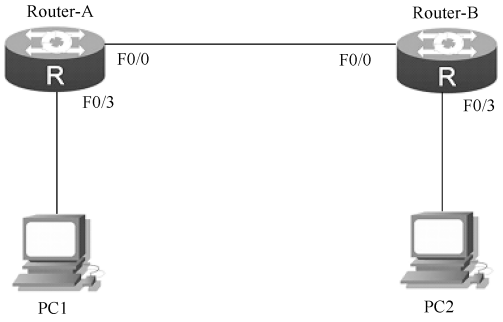


图 3-2-11　利用 RIP 实现网络连通的拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 3-2-3。

表 3-2-3　交换机和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Router-A	F0/0	192.168.1.1	255.255.255.0	无
	F0/3	192.168.10.1	255.255.255.0	无
Router-B	F0/0	192.168.1.2	255.255.255.0	无
	F0/3	192.168.20.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

相关知识

RIP 是应用较早、使用较普遍的内部网关协议，适用于小型同类网络的一个自治系统内的路由信息的传递。RIP 基于距离矢量算法。它使用“跳数”，即 metric 来衡量到达目的地址的路由距离，取值为 1～15，数值 16 表示无穷大。RIP 进程使用 UDP 的 520 端口来发送和接收 RIP 分组。RIP 分组每隔 30s 以广播的形式发送一次，为了防止出现“广播风暴”，其后续的分组将做随机延时后发送。在 RIP 中，如果一个路由在 180s 内未被刷新，则相应的距离被设定成无穷大，并从路由表中删除该表项。

使用距离矢量路由协议的路由器并不了解到达目的网络的整条路径。距离矢量协议将路由器作为通往最终目的地的路径上的路标。路由器唯一了解的远程网络信息就是到该网络的距离（度量）及可通过哪条路径或哪个接口到达该网络。 距离矢量路由协议并不了解确切的网络拓扑图。

有两个距离矢量 IPv4 IGP，即 RIPv1 —— 第一代传统协议、RIPv2 —— 简单距离矢量路由协议。

RIPv1 被提出较早，其中有许多缺陷。为了改善 RIPv1 的不足，在 RFC 1388 中提出了改进的 RIPv2，并在 RFC 1723 和 RFC 2453 中进行了修订。RIPv2 定义了一套有效的改进方案，新的 RIPv2 支持子网路由选择，支持 CIDR，支持组播，并提供了验证机制。其区别见表 3-2-4。

表 3-2-4 RIPv1 和 RIPv2 的区别

RIPv1	RIPv2
有类路由协议	无类路由协议
不能支持 VLSM	可以支持 VLSM
没有认证的功能	可以支持认证，并且有明文和 MD5 两种认证
手工汇总的功能	可以在关闭自动汇总的前提下，进行手工汇总
广播更新 255.255.255.255	组播更新 224.0.0.9

在三层交换机上 RIP 动态路由协议的配置命令如下：

```
router#config
Switch_config#router rip    !启动RIP路由协议
Switch config router#network network
Switch(config-router)#
```

步骤实现

步骤 1：按照图 3-2-11 连接网络拓扑结构。

步骤 2：按照表 3-2-4 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
Router>enable                                          !进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          !删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          !重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router>enable
Router#config
Router_config#hostname Router-A
Router-A config#interface Fastethernet 0/0
Router-A config f0/0#ip address 192.168.1.1 255.255.255.0
Router-A_config#interface Fastethernet 0/3
Router-A_config_f0/3#ip address 192.168.10.1  255.255.255.0
```

步骤 5：查看 Router-A 的接口 IP 地址配置情况。

```
Router-A#show ip int brief
Interface               IP-Address        Method    Protocol-Status
Async0/0                unassigned         manual        down
Serial0/1               unassigned         manual        down
Serial0/2               unassigned         manual        down
FastEthernet0/0          192.168.1.1       manual        up
FastEthernet0/3          192.168.10.1      manual        up
```

```
Router-A#
```

步骤 6：配置 Router-B 的名称及其接口 IP 地址。

```
Router>enable
Router#config
Router config#hostname Router-B
Router-B config#interface Fastethernet 0/0
Router-B_config_f0/0#ip address 192.168.1.2  255.255.255.0
Router-B config#interface Fastethernet 0/3
Router-B_config_f0/3#ip address 192.168.20.1  255.255.255.0
```

步骤 7：查看 Router-B 的接口 IP 地址配置情况。

```
Router-B#show ip int brief
Interface               IP-Address         Method    Protocol-Status
Async0/0                unassigned         manual          down
Serial0/1               unassigned         manual          down
Serial0/2               unassigned         manual          down
FastEthernet0/0          192.168.1.2       manual          up
FastEthernet0/3          192.168.20.1      manual          up
Router-B#
```

步骤 8：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.10.0/24     is directly connected, FastEthernet0/3
Router-A#
```

步骤 9：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.20.0/24     is directly connected, FastEthernet0/3
Router-B#
```

步骤 10：配置路由协议前，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络不连通，如图 3-2-12 所示。

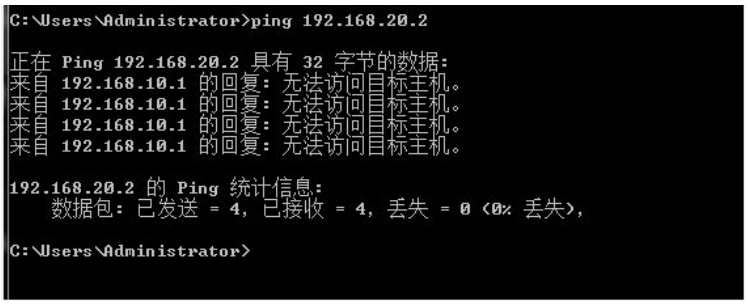


图 3-2-12　连通性测试效果图（一）

（2）在 PC2 上 ping 192.168.10.2，网络不连通，如图 3-2-13 所示。

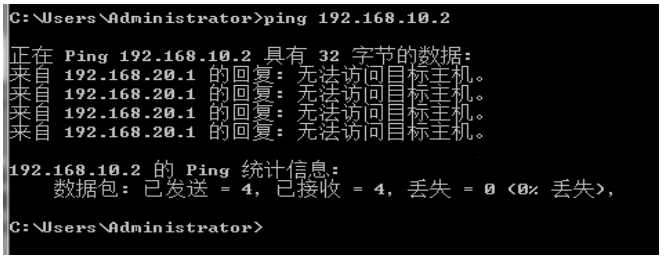


图 3-2-13　连通性测试效果图（二）

步骤 11：在 Router-A 上配置 RIPv1 协议。

```
Router-A_config#router rip                          ! 启动RIP
Router-A_config_rip #network 192.168.10.0           ! 宣告直连网段
Router-A_config_rip #network 192.168.1.0            ! 宣告直连网段
```

步骤 12：在 Router-B 上配置 RIPv1 协议。

```
Router-B _config#router rip                         ! 启动RIP协议
Router- B _config_rip #network 192.168.1.0          ! 宣告直连网段
Router- B _config_rip #network 192.168.20.0         ! 宣告直连网段
```

步骤 13：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      192.168.1.0/24       is directly connected, FastEthernet0/0
C      192.168.10.0/24      is directly connected, FastEthernet0/3
R      192.168.20.0/24      [120,1] via 192.168.1.2(on FastEthernet0/0)
                                ! 从Router-B学习到的路由，类型为R
```

步骤 14：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      192.168.1.0/24       is directly connected, FastEthernet0/0
C      192.168.20.0/24      is directly connected, FastEthernet0/3
R      192.168.10.0/24      [120,1] via 192.168.1.1(on FastEthernet0/0)
  ! 从Router-A学习到的路由，类型为R
Router-B#
```

步骤 15：配置路由协议后，验证网络的连通性。

（1）在 PC1 上 ping 192.168.20.2，网络已连通，如图 3-2-14 所示。

图 3-2-14　连通性测试效果图（三）

（2）在 PC2 上 ping 192.168.10.2，网络已连通，如图 3-2-15 所示。

图 3-2-15　连通性测试效果图（四）

小贴士

（1）只能宣告直连的网段。

（2）宣告时不附加掩码。

（3）分配的地址最好是连续的子网，以免 RIP 汇聚时出现错误。

知识拓展

RIPv2 动态路由协议的实现：RIPv2 定义了一套有效的改进方案，新的 RIPv2 支持子网路由选择，支持 CIDR，支持组播，并提供了验证机制。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）PC 2 台。

（3）交叉线 3 条。

（4）Console 线 1 条。

利用 RIP 实现网络连通的拓扑结构如图 3-2-16 所示。

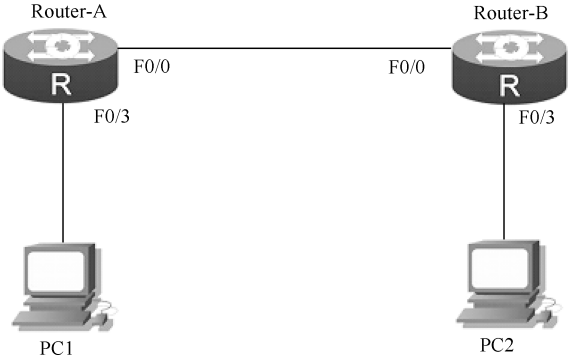


图 3-2-16　利用 RIP 实现网络连通的拓扑结构

路由器和 PC 的 IP 地址网络参数设置见表 3-2-5。

表 3-2-5　路由器和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Router-A	F0/0	172.16.1.1	255.255.255.0	无
	F0/3	172.16.0.1	255.255.255.0	无
Router-B	F0/0	172.16.1.2	255.255.255.0	无
	F0/3	172.16.2.1	255.255.255.0	无
PC1		172.16.0.2	255.255.255.0	172.16.0.1
PC2		172.16.2.2	255.255.255.0	172.16.2.1

步骤实现

步骤 1：按照图 3-2-16 连接网络拓扑结构。

步骤 2：按照表 3-2-5 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
    Router>enable                                          ！进入特权模式
    Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
```

```
Router#delete                                          ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router_config#hostname Router-A
Router-A config#interface Fastethernet 0/0
Router-A config f0/0#ip address 172.16.1.1 255.255.255.0
Router-A_config#interface Fastethernet 0/3
Router-A_config_f0/3#ip address 172.16.0.1  255.255.255.0
```

步骤 5：查看 Router-A 的接口 IP 地址配置情况。

```
Router-A#show ip int b
Interface               IP-Address      Method    Protocol-Status
Async0/0                unassigned       manual         down
Serial0/1               unassigned       manual         down
Serial0/2               unassigned       manual         down
FastEthernet0/0          172.16.1.1      manual         up
FastEthernet0/3          172.16.0.1      manual         up
```

步骤 6：配置 Router-B 的名称及其接口 IP 地址。

```
Router config#hostname Router-B
Router-B_config#interface Fastethernet 0/0
Router-B config f0/0#ip address 172.16.1.2  255.255.255.0
Router-B config#interface Fastethernet 0/3
Router-B_config_f0/3#ip address 172.16.2.1  255.255.255.0
```

步骤 7：查看 Router-B 的接口 IP 地址配置情况。

```
Router-B#show ip int brief
Interface               IP-Address      Method    Protocol-Status
Async0/0                unassigned      manual         down
Serial0/1               unassigned      manual         down
Serial0/2               unassigned      manual         down
FastEthernet0/0          172.16.1.2     manual         up
FastEthernet0/3          172.16.2.1     manual         up
Router-B#
```

步骤 8：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0
```

```
C     172.16.1.0/24       is directly connected, FastEthernet0/0
C     172.16.0.0/24       is directly connected, FastEthernet0/3
Router-A#
```

步骤 9：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     172.16.1.0/24       is directly connected, FastEthernet0/0
C     172.16.2.0/24       is directly connected, FastEthernet0/3
```

步骤 10：配置路由协议前，验证网络的连通性。

（1）在 PC1 上 ping 172.16.0.2，网络不连通，如图 3-2-17 所示。

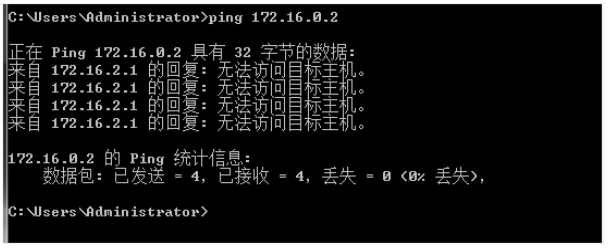


图 3-2-17　连通性测试效果图（一）

（2）在 PC2 上 ping 172.16.2.2，网络不连通，如图 3-2-18 所示。

图 3-2-18　连通性测试效果图（二）

步骤 11：在 Router-A 上配置 RIPv2 协议并关闭自动汇总。

```
Router-A_config#router rip                          ! 启动RIP
Router-A_config_rip#version 2                       ! 指明为版本2
Router-A_config_rip#no auto-summary                 ! 关闭自动汇总
Router-A_config_rip #network 172.16.1.0             ! 宣告直连网段
Router-A_config_rip #network 172.16.0.0             ! 宣告直连网段
```

步骤 12：在 Router-B 上配置 RIPv2 协议并关闭自动汇总。

```
Router-B _config#router rip                         ! 启动RIP协议
Router- B _config_rip#version 2                     ! 指明为版本2
```

```
Router- B _config_rip#no auto-summary                ！关闭自动汇总
Router- B _config_rip #network 172.16.2.0            ！宣告直连网段
Router- B _config_rip #network 172.16.1.0            ！宣告直连网段
```

步骤 13：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      172.16.0.0/24       is directly connected, FastEthernet0/3
C      172.16.1.0/24       is directly connected, FastEthernet0/0
R      172.16.2.0/24       [120,1] via 172.16.1.2(on FastEthernet0/0)
Router-A#
！从Router-B学习到的路由，类型为R
```

步骤 14：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

R      172.16.0.0/24       [120,1] via 172.16.1.1(on FastEthernet0/0)
C      172.16.1.0/24       is directly connected, FastEthernet0/0
C      172.16.2.0/24       is directly connected, FastEthernet0/3
Router-B#
            ！从Router-A学习到的路由，类型为R
```

步骤 15：配置路由协议后，验证网络的连通性。

（1）在 PC1 上 ping 172.16.2.2，网络已连通，如图 3-2-19 所示。

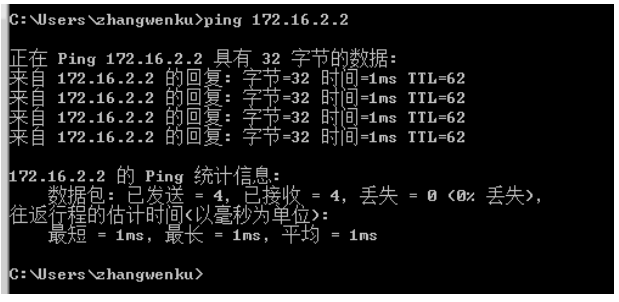


图 3-2-19　连通性测试效果图（三）

（2）在 PC2 上 ping 172.16.0.2，网络已连通，如图 3-2-20 所示。

图 3-2-20　连通性测试效果图（四）

小贴士

如果不使用 RIPv2 路由协议，则会导致计算机之间在使用 ping 命令的时候丢包。

学习小结

本学习活动介绍了路由器之间如何实现 RIP 路由，需要注意的是 RIP 协议有两个版本，即 RIPv1 和 RIPv2，no auto-summary 功能只支持 RIPv2。路由器只宣告自己的直连网段，实现动态更新路由。

学习活动 3　路由器的 OSPF 动态路由配置

OSPF 协议是目前网络中应用最广泛的动态路由协议之一，也属于内部网关路由协议，能够适应各种规模的网络环境，是典型的链路状态协议。

学习情境

公司的规模越来越大，路由器的数量也逐渐增多，已经达到了 8 台。该公司的网络管理员经过考虑，发现原有的 RIP 路由协议也已不再适合现有公司的应用了。因此，决定在公司的路由器之间使用动态的 OSPF 路由协议，实现网络的互连。

情境分析

由于公司的网络规模越来越大，管理员发现使用 OSPF 路由协议再适合不过了，因为 OSPF 路由协议可以实现快速的收敛，并且出现环路的可能性不大，因此适用于中大型企业网络。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）PC 2 台。

（3）交叉线 3 条。

配置 OSPF 协议单区域拓扑结构如图 3-2-21 所示。

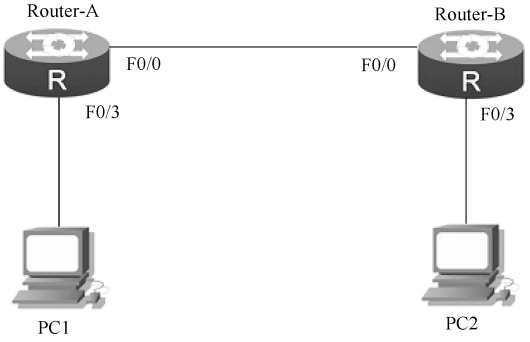


图 3-2-21　配置 OSPF 协议单区域拓扑结构

路由器和 PC 的 IP 地址网络参数设置见表 3-2-6。

表 3-2-6　路由器和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关
Router-A	F0/0	172.16.1.1	255.255.255.0	无
	F0/3	172.16.0.1	255.255.255.0	无
Router-B	F0/0	172.16.1.2	255.255.255.0	无
	F0/3	172.16.2.1	255.255.255.0	无
PC1		172.16.0.2	255.255.255.0	172.16.0.1
PC2		172.16.2.2	255.255.255.0	172.16.2.1

相关知识

OSPF 协议是一种链路状态路由协议，旨在替代距离矢量路由协议。RIP 是网络和 Internet 早期广为接受的路由协议。但是，RIP 依靠跳数作为确定最佳路由的唯一度量，很快便出现了问题。在拥有速度各异的多条路径的大型网络中，使用跳数无法很好地扩展。OSPF 与 RIP 相比具有巨大优势，因为它既能快速收敛，又能扩展到更大型的网络。

要创建 OSPF 路由进程，在全局命令配置模式下，执行以下命令：

```
router#config
router_config#router ospf process-id    !启动OSPF路由进程
router config router process-id#network network netmask  area
area-id   !定义接口所属区域
router_config_router_process-id#
```

说明：进程号的数值为 1～65535，在网络中每台路由器上的进程号可以相同也可以不同。神州数码路由器中，在使用 OSPF 路由协议时，network 后面跟的是直连网段和相应的子网掩码，这一点和其他品牌的路由器有所区别，需要特别注意。

步骤实现

步骤 1：按照图 3-2-21 连接网络拓扑结构。

步骤 2：按照表 3-2-6 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router_config#hostname Router-A
Router-A config#interface Fastethernet 0/0
Router-A config f0/0#ip address 172.16.1.1 255.255.255.0
Router-A_config#interface Fastethernet 0/3
Router-A_config_f0/3#ip address 172.16.0.1  255.255.255.0
```

步骤 5：查看 Router-A 的接口 IP 地址配置情况。

```
Router-A#show ip int brief
Interface               IP-Address     Method    Protocol-Status
Async0/0                unassigned     manual          down
Serial0/1               unassigned     manual          down
Serial0/2               unassigned     manual          down
FastEthernet0/0         172.16.1.1     manual          up
FastEthernet0/3         172.16.0.1     manual          up
```

步骤 6：配置 Router-B 的名称及其接口 IP 地址。

```
Router config#hostname Router-B
Router-B config#interface Fastethernet 0/0
Router-B_config_f0/0#ip address 172.16.1.2  255.255.255.0
Router-B config#interface Fastethernet 0/3
Router-B_config_f0/3#ip address 172.16.2.1  255.255.255.0
```

步骤 7：查看 Router-B 的接口 IP 地址配置情况。

```
Router-B#show ip int brief
Interface               IP-Address      Method    Protocol-Status
Async0/0                unassigned      manual          down
Serial0/1               unassigned      manual          down
Serial0/2               unassigned      manual          down
```

```
FastEthernet0/0          172.16.1.2      manual          up
FastEthernet0/3          172.16.2.1      manual          up
Router-B#
```

步骤 8：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      172.16.1.0/24       is directly connected, FastEthernet0/0
C      172.16.0.0/24       is directly connected, FastEthernet0/3
Router-A#
```

步骤 9：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      172.16.1.0/24       is directly connected, FastEthernet0/0
C      172.16.2.0/24       is directly connected, FastEthernet0/3
```

步骤 10：配置路由协议前，验证网络的连通性。

（1）在 PC1 上 ping 172.16.0.2，网络不连通，如图 3-2-22 所示。

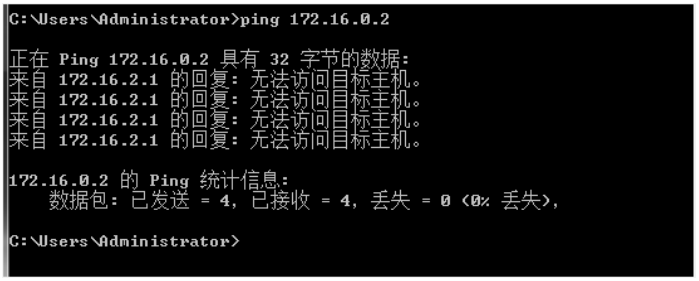


图 3-2-22　连通性测试效果图（一）

（2）在 PC2 上 ping 172.16.2.2，网络不连通，如图 3-2-23 所示。

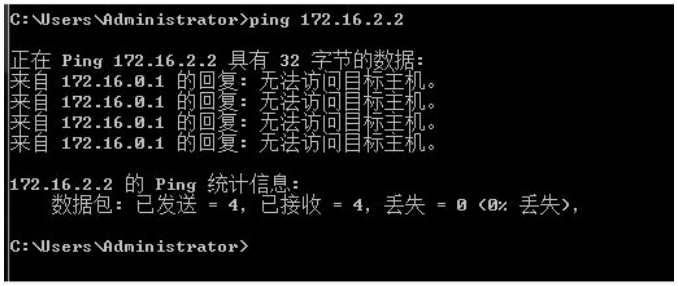


图 3-2-23　连通性测试效果图（二）

步骤 11：在 Router-A 上配置 OSPF 路由协议。

```
Router-A config#router ospf  1
Router-A_config_ospf_1#network 172.16.0.0 255.255.255.0 area 0
Router-A config ospf 1#network 172.16.1.0 255.255.255.0 area 0
Router-A_config#router ospf  1#
```

步骤 12：在 Router-B 上配置 OSPF 路由协议。

```
Router-B_config#router ospf  1
Router-B config ospf 1#network 172.16.1.0  255.255.255.0 area 0
Router-B config ospf 1#network 172.16.2.0  255.255.255.0 area 0
Router-B_config_ospf_1#
```

小贴士

在配置 OSPF 协议通告相应网络时要确保子网掩码配置正确，且要说明路由器所在的区域。

步骤 13：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      172.16.0.0/24       is directly connected, FastEthernet0/3
C      172.16.1.0/24       is directly connected, FastEthernet0/0
O      172.16.2.0/24       [110,2] via 172.16.1.2(on FastEthernet0/0)
Router-A#
```

步骤 14：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
```

```
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

O      172.16.0.0/24        [110,2] via 172.16.1.1(on FastEthernet0/0)
C      172.16.1.0/24        is directly connected, FastEthernet0/0
C      172.16.2.0/24        is directly connected, FastEthernet0/3
Router-B#
```

步骤 15：验证网络的连通性。

（1）在 PC1 上 ping 172.16.0.2，网络已连通，如图 3-2-24 所示。

图 3-2-24　连通性测试效果图（三）

（2）在 PC2 上 ping 172.16.2.2，网络已连通，如图 3-2-25 所示。

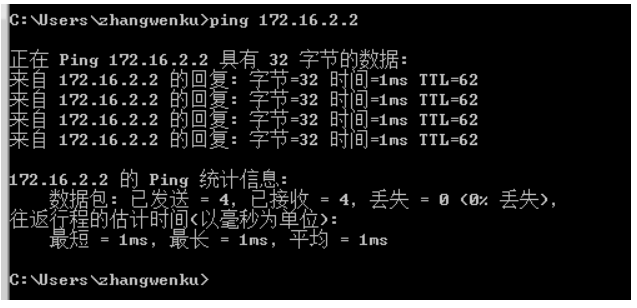


图 3-2-25　连通性测试效果图（四）

小贴士

（1）每个路由器的 OSPF 进程号可以不同，一个路由器可以有多个 OSPF 进程。

（2）OSPF 是无类路由协议，一定要加子网掩码。

（3）第一个区域必须是区域 0。

知识拓展

OSPF 动态路由协议多区域的实现：对于复杂的网络，OSPF 协议可使用多个区域以分层方式实施。所有区域必须连接到主干区域（区域 0）。互连各个区域的路由器称为区域边界路

由器（ABR）。

利用多区域 OSPF，OSPF 可以把一个大型自治系统划分为更小的区域，以支持分层路由。采用分层路由后，各个区域之间仍然能够进行路由（区域间路由），但许多处理器密集型的路由操作（如重新计算数据库）在区域内进行。

例如，每当路由器收到与区域中拓扑更改有关的最新信息时（包括添加、删除或修改链路），路由器必须重新运行 SPF 算法，创建新的 SPF 树并更新路由表。SPF 算法会占用很多 CPU 资源，且其耗费的计算时间取决于区域大小。

注意：拓扑更改以距离矢量格式分布到其他区域中的路由器。换句话说，这些路由器只会更新其路由表，无须重新运行 SPF 算法。

一个区域中有过多路由器会使 LSDB 非常大并增加 CPU 的负载。因此，将路由器有效分区可以把巨大的数据库分成更小、更易管理的数据库。

多区域 OSPF 的分层拓扑具有以下优势。

路由表减小——路由表条目减少，因为区域之间的网络地址可以总结。默认情况下不启用路由总结。

链路状态更新开销减少——将处理和内存要求降到最低。

SPF 计算频率降低——使拓扑变化仅影响区域内部。例如，由于 LSA 泛洪在区域边界终止，它使路由更新的影响降到最小。

所需设备：

（1）DCR-2655 路由器 3 台。

（2）PC 3 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）交叉线 4 条。

（6）Console 线 1 条。

配置 OSPF 多区域的网络拓扑结构如图 3-2-26 所示。

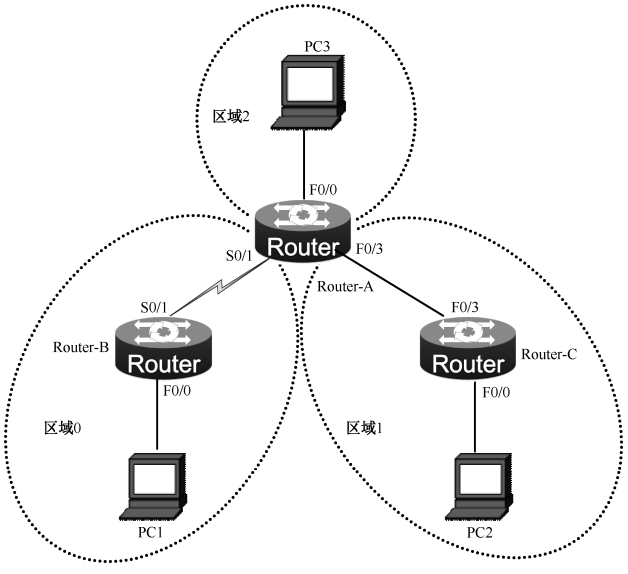


图 3-2-26　配置 OSPF 多区域的网络拓扑结构

路由器和 PC 的 IP 地址网络参数设置见表 3-2-7。

表 3-2-7　路由器和 PC 的 IP 地址网络参数设置

设　备	端　口	IP 地址	子网掩码	网　关	所属区域
Router-A	S0/1	192.168.4.1	255.255.255.0	无	0
	F0/0	192.168.3.1	255.255.255.0	无	2
	F0/3	192.168.5.1	255.255.255.0	无	1
Router-B	S0/1	192.168.4.2	255.255.255.0	无	0
	F0/0	192.168.1.1	255.255.255.0	无	0
Router-C	F0/0	192.168.2.1	255.255.255.0	无	1
	F0/3	192.168.5.2	255.255.255.0	无	1
PC1		192.168.1.2	255.255.255.0	192.168.1.1	0
PC2		192.168.2.2	255.255.255.0	192.168.2.1	1
PC3		192.168.3.2	255.255.255.0	192.168.3.1	2

步骤 1：按照图 3-2-26 连接网络拓扑结构。

步骤 2：按照表 3-2-7 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router config#hostname Router-A
Router-A config#int fa0/0
Router-A config f0/0#ip add 192.168.3.1 255.255.255.0
Router-A config f0/0#no shutdown
Router-A config f0/0#interface serial 0/1
Router-A config s0/1# physical-layer speed 2048000
Router-A config s0/1#ip address 192.168.4.1  255.255.255.0
Router-A config s0/1#no shutdown
Router-A config s0/1#int fa0/3
Router-A config f0/3#ip add 192.168.5.1 255.255.255.0
Router-A config f0/3#no shutdown
Router-A config f0/3#^Z
Router-A#
```

步骤 5：查看 Router-A 的接口 IP 地址配置情况。

```
Router-A#show ip int brief
```

```
Interface              IP-Address     Method    Protocol-Status
Async0/0               unassigned     manual         down
Serial0/1              192.168.4.1    manual         up
Serial0/2              unassigned     manual         down
FastEthernet0/0        192.168.3.1    manual         up
FastEthernet0/3        192.168.5.1    manual         up
Router-A#
```

步骤 6：配置 Router-B 的名称及其接口 IP 地址。

```
Router config#hostname Router-B
Router-B_config#int fa0/0
Router-B config f0/0#ip add 192.168.1.1 255.255.255.0
Router-B_config_f0/0#no shutdown
Router-B config f0/0#interface serial 0/1
Router-B config s0/1# physical-layer speed 2048000
Router-B_config_s0/1#ip address 192.168.4.2  255.255.255.0
Router-B config s0/1#no shutdown
Router-B config s0/1#^Z
Router-B#
```

步骤 7：查看 Router-B 的接口 IP 地址配置情况。

```
Router-B#show ip int brief
Interface              IP-Address     Method    Protocol-Status
Async0/0               unassigned     manual         down
Serial0/1              192.168.4.2    manual         up
Serial0/2              unassigned     manual         down
FastEthernet0/0        192.168.1.1    manual         up
FastEthernet0/3        unassigned     manual         down
Router-B#
```

步骤 8：配置 Router-C 的名称及其接口 IP 地址。

```
Router config#hostname Router-C
Router-C config#int fa0/0
Router-C_config_f0/0#ip add 192.168.2.1 255.255.255.0
Router-C config f0/0#no shutdown
Router-C config f0/0#int fa0/3
Router-C_config_f0/3#ip add 192.168.5.2 255.255.255.0
Router-C config f0/3#no shutdown
Router-C config f0/3#^Z
Router-C#
```

步骤 9：查看 Router-C 的接口 IP 地址配置情况。

```
Router-C#show ip int brief
Interface              IP-Address     Method    Protocol-Status
Async0/0               unassigned     manual         down
Serial0/1              unassigned     manual         down
Serial0/2              unassigned     manual         down
FastEthernet0/0        192.168.2.1    manual         up
```

```
FastEthernet0/3          192.168.5.2    manual         up
Router-C#
```

步骤 10：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.3.0/24      is directly connected, FastEthernet0/0
C     192.168.4.0/24      is directly connected, Serial0/1
Router-A#
```

步骤 11：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.1.0/24      is directly connected, FastEthernet0/0
C     192.168.4.0/24      is directly connected, Serial0/1
C     192.168.5.0/24      is directly connected, FastEthernet0/3
Router-B#
```

步骤 12：查看 Router-C 的路由表。

```
Router-C#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.2.0/24      is directly connected, FastEthernet0/0
C     192.168.5.0/24      is directly connected, FastEthernet0/3
Router-C#
```

步骤 13：配置路由协议前，验证网络的连通性。

（1）在 PC1 上 ping 192.168.2.2 和 192.168.3.2，网络不连通，如图 3-2-27 所示。

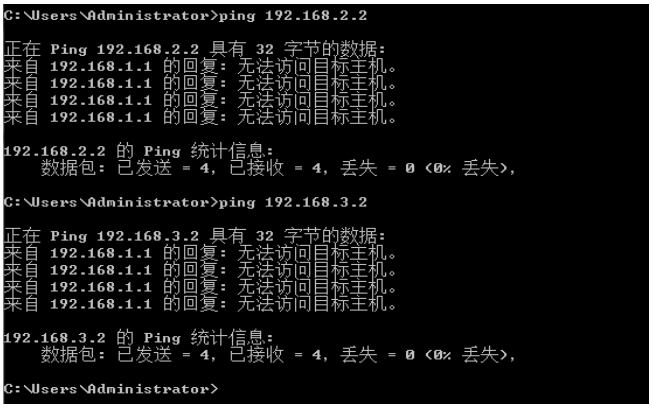


图 3-2-27　连通性测试效果图（一）

（2）在 PC2 上 ping 192.168.1.2 和 192.168.3.2，网络不连通，如图 3-2-28 所示。

图 3-2-28　连通性测试效果图（二）

（3）在 PC3 上 ping 192.168.1.2 和 192.168.2.2，网络不连通，如图 3-2-29 所示。

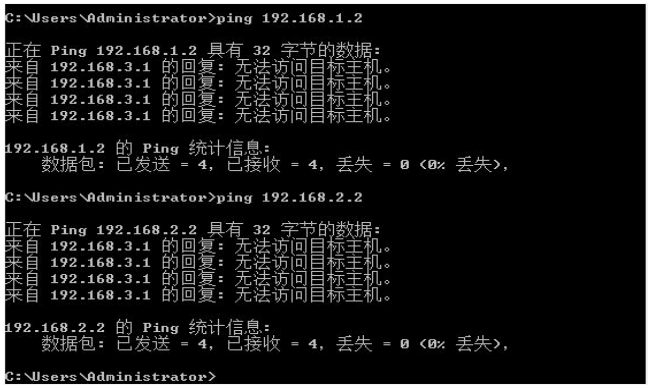


图 3-2-29　连通性测试效果图（三）

步骤 14：在 Router-A 上配置 OSPF 的多区域。

```
Router-A#config
Router-A config#router ospf 1
Router-A config ospf 1#network 192.168.3.0 255.255.255.0 area 2
Router-A_config_ospf_1#network 192.168.4.0 255.255.255.0 area 0
Router-A_config_ospf_1#network 192.168.5.0 255.255.255.0 area 1
```

```
Router-A_config_ospf_1#
```

步骤 15：在 Router-B 上配置 OSPF 的多区域。

```
Router-B#config
Router-B_config#router ospf 1
Router-B config ospf 1#network 192.168.1.0 255.255.255.0 area 0
Router-B config ospf 1#network 192.168.4.0 255.255.255.0 area 0
Router-B_config_ospf_1#
```

步骤 16：在 Router-C 上配置 OSPF 协议。

```
Router-C#config
Router-C config#router ospf 1
Router-C config ospf 1#network 192.168.2.0 255.255.255.0 area 1
Router-C_config_ospf_1#network 192.168.5.0 255.255.255.0 area 1
Router-C_config_ospf_1#
```

步骤 17：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

O      192.168.1.0/24       [110,1601] via 192.168.4.2(on Serial0/1)
O      192.168.2.0/24       [110,2] via 192.168.5.2(on FastEthernet0/3)
C      192.168.3.0/24       is directly connected, FastEthernet0/0
C      192.168.4.0/24       is directly connected, Serial0/1
C      192.168.5.0/24       is directly connected, FastEthernet0/3
Router-A#
```

步骤 18：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      192.168.1.0/24       is directly connected, FastEthernet0/0
O IA   192.168.2.0/24        [110,1602] via 192.168.4.1(on Serial0/1)
O IA   192.168.3.0/24        [110,1601] via 192.168.4.1(on Serial0/1)
C      192.168.4.0/24       is directly connected, Serial0/1
O IA   192.168.5.0/24        [110,1601] via 192.168.4.1(on Serial0/1)
```

```
Router-B#
```

步骤 19：查看 Router-C 的路由表。

```
Router-C#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

O IA   192.168.1.0/24      [110,1602] via 192.168.5.1(on FastEthernet0/3)
C      192.168.2.0/24      is directly connected, FastEthernet0/0
O IA   192.168.3.0/24      [110,2] via 192.168.5.1(on FastEthernet0/3)
O IA   192.168.4.0/24      [110,1601] via 192.168.5.1(on FastEthernet0/3)
C      192.168.5.0/24      is directly connected, FastEthernet0/3
Router-C#
```

步骤 20：配置路由协议后，验证网络的连通性。

（1）在 PC1 上 ping 192.168.2.2 和 192.168.3.2，网络已连通，如图 3-2-30 所示。

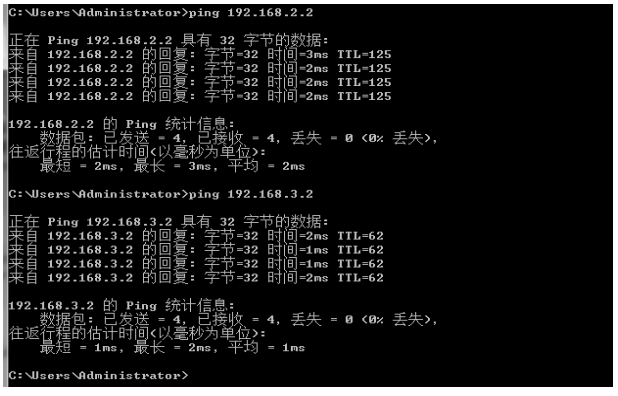


图 3-2-30　连通性测试效果图（四）

（2）在 PC2 上 ping 192.168.1.2 和 192.168.3.2，网络已连通，如图 3-2-31 所示。

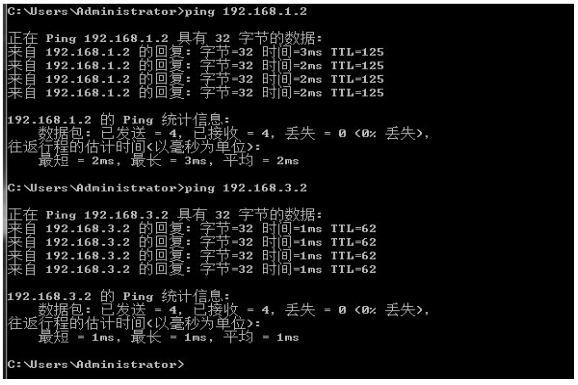


图 3-2-31　连通性测试效果图（五）

（3）在 PC3 上 ping 192.168.1.2 和 192.168.2.2，网络已连通，如图 3-2-32 所示。

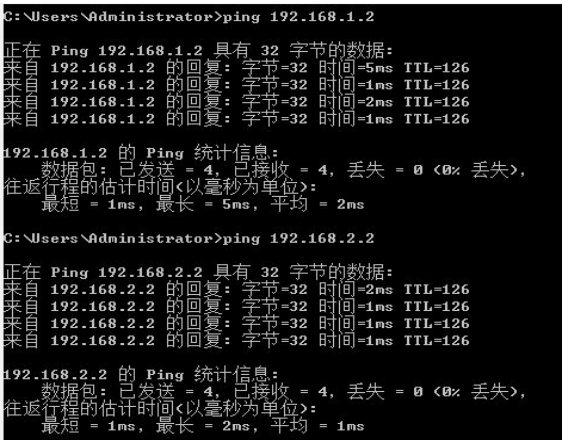

C:\Users\Administrator>ping 192.168.1.2
正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间=5ms TTL=126
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.2 的回复: 字节=32 时间=2ms TTL=126
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=126
192.168.1.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 1ms, 最长 = 5ms, 平均 = 2ms
C:\Users\Administrator>ping 192.168.2.2
正在 Ping 192.168.2.2 具有 32 字节的数据:
来自 192.168.2.2 的回复: 字节=32 时间=2ms TTL=126
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=126
192.168.2.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 1ms, 最长 = 2ms, 平均 = 1ms

图 3-2-32　连通性测试效果图（六）

小贴士

在配置 OSPF 多区域时，骨干区域（area 0）只有一个，且要为每个路由器指定所在的区域。

学习小结

本学习活动介绍了路由器之间如何实现动态路由 OSPF 协议，使用 OSPF 路由协议宣告直连网段时，需要使用该网段的子网掩码，而且必须指明所属的区域。

项目考核

1．飞翔公司规模很小，只有一家总公司和一家上海分公司，经理决定组建一个网络实现总公司和分公司的通信，公司网管经过分析，决定使用静态路由协议，如图 3-2-33 所示。

（1）先用静态路由实现全网互通。

（2）将静态路由清除，用 RIPv2 实现全网互通，注意三层交换机的配置。

完成标准：各网段能相互通信。

2．配置 OSPF 单区域。蓝翔公司有两个分公司，它们的子网分别为 172.16.4.0/24、172.16.5.0/24，服务器群的地址为 172.16.3.0/24，为了节省 IP 地址，公司采用了 VLSM，为了便于管理，公司网管采用了 OSPF 动态路由协议，如图 3-2-34 所示。

完成标准：各网段能相互通信。

3．配置 OSPF 多区域。天翔公司总部设在美国，中国分公司网络通过路由器 RA 接入总部网络，加拿大分公司通过路由器 RB 接入总部网络。由于公司网络规模较大且设备的厂商不同，为了解决路由收敛速度和设备厂商兼容性的问题，该公司的网管打算采用链路状态路由协议实现路由选择，如图 3-2-35 所示。

完成标准：各网段能相互通信。

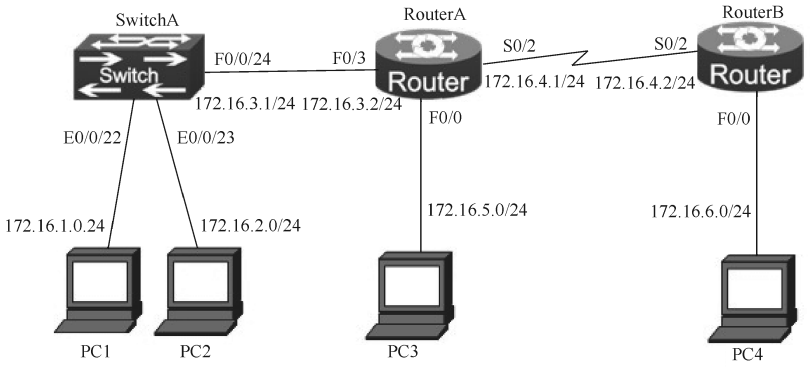


图 3-2-33　飞翔公司网络拓扑结构

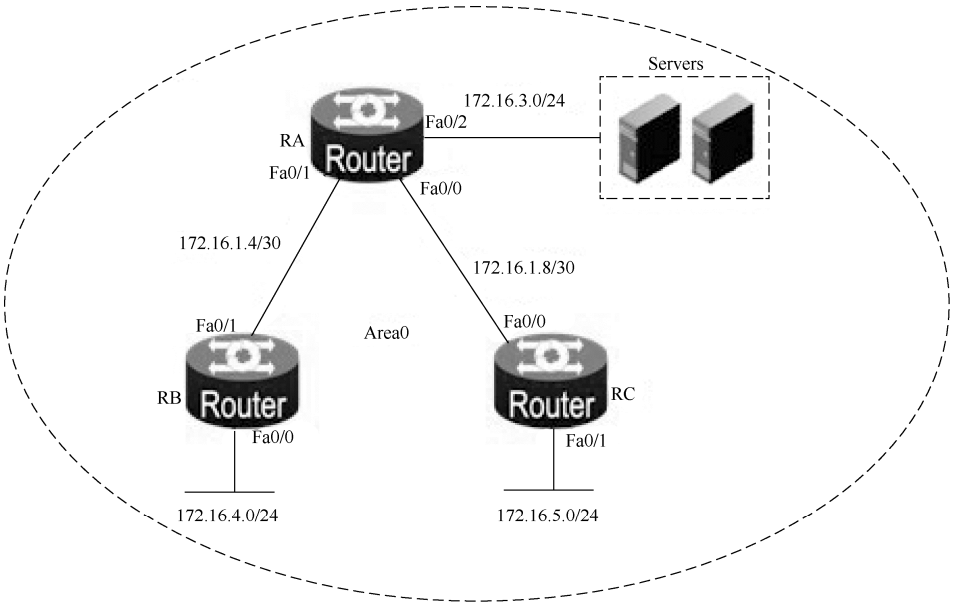


图 3-2-34　蓝翔公司网络拓扑结构

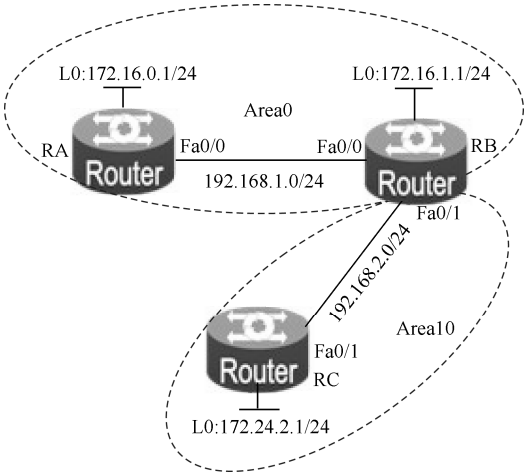
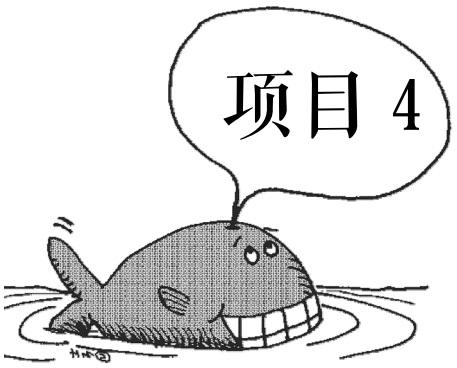


图 3-2-35　天翔公司网络拓扑结构



网络的安全配置

项目学习说明

由于网络的迅猛发展，网络安全已成为网络发展的一个重要议题。企业网络的安全问题也日益突出，忽视了网络设备的安全设置，就如同整个网络敞开了大门。通过针对性的设置可以使它变成一堵安全的“墙”。

本项目重点学习交换机的端口安全配置和 IP 访问控制列表配置。

学习能力目标

学习任务 1　交换机的端口安全配置

学习任务 2　IP 访问控制列表配置

职业能力目标

- 能实现交换机的端口安全配置
- 能理解 IP 访问控制列表的工作机制与特点
- 能实现几种常用的 IP 访问控制列表的配置

学习任务 1　端口安全配置

在日常工作中，网络管理员经常遇到单位员工计算机中毒的情况，如冲击波病毒可造成整个园区网络速度变慢，甚至瘫痪。虽然通过数据流监控软件可以分析出中毒计算机的 MAC 地址，但由于并未做相关的设置，所以出现问题时查找、定位问题主机很困难，这给网络管理带来很大的麻烦。通过将 MAC 地址与端口进行绑定可以很快定位出现问题的机器。本任务分以下两个学习活动进行学习。

学习活动 1　交换机的端口安全。

学习活动 2　实现 AM 功能。

学习活动 1　交换机的端口安全

通过 MAC 地址表可记录连接到交换机端口的以太网 MAC 地址（网卡号），并只允许某个 MAC 地址通过本端口通信。其他 MAC 地址发送的数据包通过此端口时，端口安全特性会阻止它进入。

学习情境

某公司网络管理员接到单位员工计算机中病毒的电话，但查找、定位问题主机很困难，这给网络管理带来很大的麻烦，于是网络管理员决定采用 MAC 地址与端口、绑定来进行管理。

情境分析

为了安全和方便管理，可将 MAC 地址与端口进行绑定，在 MAC 地址与端口绑定后，该 MAC 地址的数据流只能从绑定端口进入，不能从其他端口进入，该端口可以允许其他 MAC 地址的数据流通过。这样，一旦网络中计算机出现了问题，就能很快定位该计算机，及时采取有效措施。

本学习活动通过 MAC 地址与端口绑定技术来实现计算机的安全接入，其在交换机上完成，实施过程中应按如下几点要求操作。

（1）交换机设置管理 IP 地址为 192.168.10.100/24，PC1 的 IP 地址设置为 192.168.10.110/24，PC2 的 IP 地址设置为 192.168.10.220/24。

（2）在交换机上对 PC1 的 MAC 地址进行端口绑定。

（3）将 PC1 分别连接到绑定的端口和未绑定的端口，并使用 ping 命令测试是否能连通交换机的 IP 地址，检验理论是否和实验一致。

（4）将 PC2 分别连接到绑定了 PC1 的 MAC 地址的端口和未绑定的端口，并使用 ping 命令测试是否能连接交换机的 IP 地址，检验理论是否和实验一致。

所需设备：

（1）DCS-3950 交换机 1 台。

（2）PC 1 台。

（3）Console 线 1 条。

（4）直通双绞线 1 条。

安全接入实验网络拓扑结构如图 4-1-1 所示。

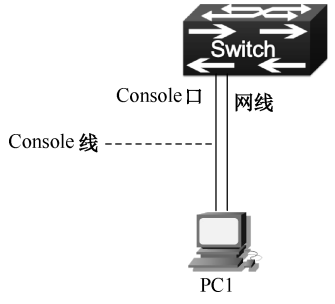


图 4-1-1　安全接入实验网络拓扑结构

相关知识

交换机的端口安全设置一般有三种方式：一是静态配置端口允许访问的主机；二是建立

基于 MAC 地址的访问控制列表；三是对 IP 地址和 MAC 地址进行一一绑定（要利用访问控制列表来实现，在后面会有介绍）。

MAC 地址或称为物理地址、硬件地址，用来定义网络设备的位置。MAC 地址是烧录在网卡中的。MAC 地址的长度是 48 位（6 字节），0～23 位称为组织唯一标志符，是识别 LAN（局域网）结点的标识，24～47 位由厂家自己分配。MAC 地址用 12 个十六进制的数字表示，如图 4-1-2 所示。

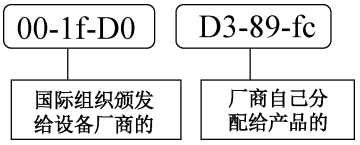


图 4-1-2　MAC 地址的结构

ipconfig 参数简介如下：

ipconfig /all：显示本机 TCP/IP 配置的详细信息；

ipconfig /release：DHCP 客户端手工释放 IP 地址；

ipconfig /renew：DHCP 客户端手工向服务器刷新请求；

ipconfig /flushdns：清除本地 DNS 缓存内容；

ipconfig /displaydns：显示本地 DNS 缓存内容；

ipconfig /registerdns：DNS 客户端手工向服务器进行注册；

ipconfig /showclassid：显示网络适配器的 DHCP 类别信息；

ipconfig /setclassid：设置网络适配器的 DHCP 类别。

步骤实现

步骤 1：按照图 4-1-1 连接网络拓扑结构。

步骤 2：交换机恢复出厂设置，配置交换机管理地址。

```
Switch#set default                                          !恢复出厂设置
Switch#write                                                !保存
Switch#reload                                               !重新启动交换机
Switch>enable                                               !进入特权模式
Switch#configuration terminal                               !进入全局配置模式
Switch(config)#interface vlan 1                             !进入管理VLAN1
Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
                                                            !设置VLAN1的IP地址
Switch(Config-if-Vlan1)#no shutdown                         !开启端口
Switch(Config-if-Vlan1)#exit                                !退出VLAN1接口
Switch(Config)#
```

步骤 3：获取 PC1 的 MAC 地址。

（1）执行“开始”→“运行”命令，弹出“运行”对话框，如图 4-1-3 所示。

（2）在“运行”对话框的“打开”文本框中输入“cmd”，如图 4-1-4 所示，按“确定”按钮，弹出命令行窗口。

图 4-1-3　执行“运行”命令

图 4-1-4　输入“cmd”命令

（3）输入“ipconfig/all”命令，查看 MAC 地址，如图 4-1-5 所示。

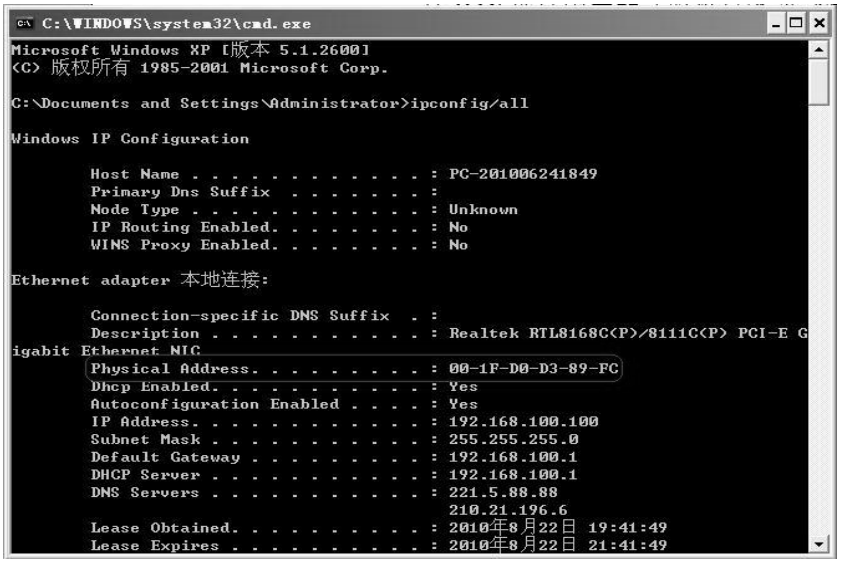

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig/all
Windows IP Configuration
Host Name . . . . . : PC-201006241849
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E Gigabit Ethernet NIC
Physical Address. . . . . : 00-1F-D0-D3-89-FC
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.100.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DHCP Server . . . . . : 192.168.100.1
DNS Servers . . . . . : 221.5.88.88
210.21.196.6
Lease Obtained. . . . . : 2010年8月22日 19:41:49
Lease Expires . . . . . : 2010年8月22日 21:41:49

图 4-1-5　查看 MAC 地址

步骤 4：开启端口 1 的 MAC 地址绑定功能。

```
Switch(config)#interface Ethernet 0/0/1                          ！进入端口1
Switch(Config-If-Ethernet0/0/1)#switchport port-security         ！开启端口安全
Switch(Config-If-Ethernet0/0/1)#
```

步骤 5：添加端口静态安全 MAC 地址，默认端口最大安全 MAC 地址数为 1。

```
Switch(Config-If-Ethernet0/0/1)#switchport port-security mac-address
00-1f-d0-d3-89-fc                ！在端口1上绑定静态MAC地址
```

用如下命令验证配置：

```
Switch#show port-security                                        ！查看端口安全
Switch#show port-security mac-address                            ！查看绑定的MAC地址
```

步骤 6：使用 ping 命令验证实验结果，见表 4-1-1。

表 4-1-1　连通性验证表

PC	端　口	ping	结　果	原　因
PC1	0/0/1	192.168.1.1	通	
PC1	0/0/2	192.168.1.1	不通	
PC2	0/0/1	192.168.1.1	通	
PC2	0/0/2	192.168.1.1	通	

步骤 7：在一个以太网上静态绑定多个 MAC 地址。

```
    Switch(Config-If-Ethernet0/0/1)# switchport port-security maximum 3
                              ！设置端口1上绑定的MAC地址最大值
    Switch(Config-If-Ethernet0/0/1)# switchport port-security mac-address
aa-aa-aa-11-11-11             ！在端口1上绑定静态MAC地址
    Switch(Config-If-Ethernet0/0/1)# switchport port-security mac-address
aa-aa-aa-22-22-22             ！在端口1上绑定静态MAC地址
```

小贴士

端口绑定必须在没有开启 spanning-tree、802.1x 情况下，且在没有进行端口汇聚或端口配置为 Trunk 的前提下进行，否则配置将不能成功。

知识拓展

动态实现 MAC 地址与端口绑定：为了实现园区网络的安全性，可以使用 MAC 地址绑定的办法对终端设备的接入端口进行限制，但使用手动方式静态输入 MAC 地址进行绑定在小型的网络中尚可实施，如果面对一个终端众多的网络，这种方法显然太烦琐，对网络管理员来说，这无疑是一项异常庞大的工作。因此，我们可以通过一定的设置，实现由交换机通过学习到的 MAC 地址表自动转化为配置文件中的绑定项，从而减少网络管理员手动输入的条目，也进一步避免了由此产生的配置文件失误所带来的安全隐患发生的可能性。

所需设备：

（1）DCS-5650 交换机 1 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）直通线 1 条。

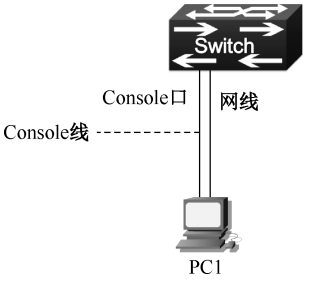


图 4-1-6　动态绑定实验网络拓扑结构

动态绑定实验网络拓扑结构如图 4-1-6 所示。

步骤 1：按照图 4-1-6 连接网络拓扑结构。

步骤 2：交换机恢复出厂设置，配置交换机管理地址。

```
    Switch#set default                                          ！恢复出厂设置
    Switch#write                                                ！保存
    Switch#reload                                               ！重新启动交换机
    Switch>enable                                               ！进入特权模式
    Switch#configuration terminal                               ！进入全局配置模式
    Switch(config)#interface vlan 1                             ！进入管理VLAN1
    Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
                                                                ！设置VLAN1的IP地址
    Switch(Config-if-Vlan1)#no shutdown                         ！开启端口
    Switch(Config-if-Vlan1)#exit                                ！退出VLAN1接口
    Switch(Config)#
```

步骤 3：获取 PC1 的 MAC 地址。

（1）执行“开始”→“运行”命令，弹出“运行”对话框。

（2）在“运行”对话框的“打开”文本框中输入“cmd”，弹出命令行窗口。

（3）输入“ipconfig/all”命令，查看 MAC 地址，如图 4-1-7 所示。

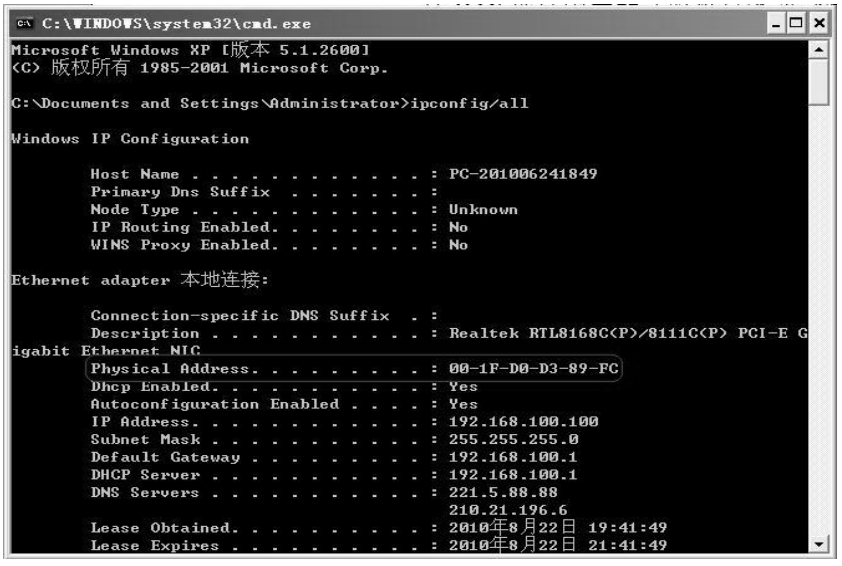

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig/all
Windows IP Configuration
Host Name . . . . . : PC-201006241849
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E G
igabit Ethernet NIC
Physical Address. . . . . : 00-1F-D0-D3-89-FC
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.100.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DHCP Server . . . . . : 192.168.100.1
DNS Servers . . . . . : 221.5.88.88
210.21.196.6
Lease Obtained. . . . . : 2010年8月22日 19:41:49
Lease Expires . . . . . : 2010年8月22日 21:41:49

图 4-1-7　查看 MAC 地址

步骤 4：启用端口 1 的 MAC 地址绑定功能，动态学习 MAC 地址并转换。

```
Switch(config)#interface Ethernet 0/0/1                    !进入端口1
Switch(Config-If-Ethernet0/0/1)#switchport port-security   !开启端口安全
Switch(Config-If-Ethernet0/0/1)# switchport port-security lock
!锁定端口
Switch(Config-If-Ethernet0/0/1)# switchport prt-security convert
                                  !设置MAC地址动态转换
Switch(Config-If-Ethernet0/0/1)#exit                       !退出端口1
```

步骤 5：验证配置。

```
Switch#show port-security address                  !查看动态转换的MAC地址
```

步骤 6：使用 ping 命令验证连通性，见表 4-1-2。

表 4-1-2　连通性验证表

PC	端　口	ping	结　果	原　因
PC1	0/0/1	192.168.1.1	通	
PC1	0/0/2	192.168.1.1	不通	
PC2	0/0/1	192.168.1.1	不通	
PC2	0/0/2	192.168.1.1	通	

小贴士

（1）当动态学习 MAC 地址无法执行“convert”命令时，请检查 PC 网卡是否和该端口正

确连接了。此命令执行后可能会出现绑定不成功的错误提示，此时需要使用“no”命令取消锁定操作，并确认端口已经学习到地址后再重新锁定和转换。

（2）端口锁定之后，该端口的 MAC 地址学习功能被关闭，不允许其他的 MAC 地址进入该端口。

（3）MAC 地址存储在地址表中有一个老化时间，它从一个地址记录加入地址表以后开始计时，如果在老化时间内各端口未收到源地址为该 MAC 地址的帧，那么，这些地址将从动态转发地址表（由源 MAC 地址、目的 MAC 地址和它们相对应的交换机的端口号组成）中被删除。静态 MAC 地址表不受地址老化时间影响。

学习小结

本学习活动实现了交换机的端口和 MAC 地址的绑定，可以使用手动方式静态绑定，也可以使用动态学习的功能进行绑定，要注意区分两种不同方法的应用场合。

学习活动 2　实现 AM 功能

AM（Access Management，访问管理）利用收到的数据报文的信息，与配置硬件地址池相比较，如果找到则转发，否则丢弃。通过对接入交换机的适当设置，可以将很多网络威胁隔离在交换机的端口内，而不会对整网产生危害。

学习情境

公司员工的计算机使用的都是固定 IP 地址，但有时员工会修改自己的 IP 地址，造成 IP 地址冲突，这样给内部网络造成了很大的麻烦，管理起来也很不方便，于是网络管理员想把计算机的 MAC 地址与 IP 地址绑定起来。

情境分析

将计算机的 MAC 地址与 IP 地址绑定起来，使用户不能随便修改 IP 地址，可以使用交换机的 AM 功能做到，网络管理员可以完善内部网络管理。AM 利用收到数据报文的信息，与配置硬件地址池相比较，如果找到则转发，否则丢弃。

通过对接入交换机的适当设置，可以将很多网络威胁隔离在交换机的端口内，而不至于对整网产生危害。

所需设备：

（1）DCRS-5650 交换机 1 台。

（2）PC 1 台。

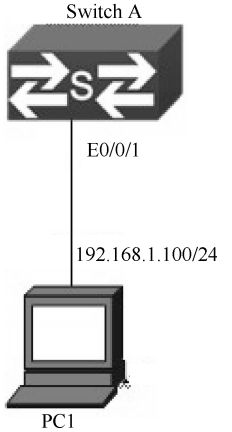


图 4-1-8　交换机与 MAC 地址绑定网络拓扑结构

（3）Console 线 1 条 。

（4）直通双绞线 1 条。

交换机与 MAC 地址绑定网络拓扑结构如图 4-1-8 所示。

相关知识

AM pool 是一个地址列表，每一个地址表项对应一个用户。每一个地址表项包括了地址信息及其对应的端口。地址信息有以下两种。

（1）IP 地址池（IP-pool），指定该端口上用户的源 IP 地址信息。

（2）MAC-IP 地址池（MAC-IP pool），指定该端口上用户的源 MAC 地址和源 IP 地址信息。

当 AM 使能的时候，AM 模块会拒绝所有的 IP 报文通过（只允许 IP 地址池内的成员源地址通过）。可以在交换机端口创建一个 MAC+IP 地址绑定，放到地址池中。当端口下连主机发送的 IP 报文（包含 ARP 报文）中所含的源 IP 地址+源 MAC 地址不符合地址池中的绑定关系时，此报文将被丢弃。

举例：使能 AM 并允许交换机接口 4 上源 IP 地址为 192.1.1.2、源 MAC 地址为 00-01-10-22-33-10 的用户通过。

```
Switch(Config)#am enable
Switch(Config)#interface Ethernet 0/0/4
Switch(Config-Ethernet0/0/4)#am port
Switch(Config-Ethernet0/0/4)#am mac-ip-pool 00-01-10-22-33-10 192.1.1.2
```

AM 的优点：配置简单，除了可以防御 ARP 攻击外，还可以防御 IP 扫描等攻击，适用于信息点不多、规模不大的静态地址环境中。

AM 的缺点：需要占用交换机的 ACL 资源，网络管理员配置量大，终端移动性差。

步骤实现

步骤 1：按照图 4-1-8 连接网络拓扑结构。

步骤 2：按照图 4-1-8 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                                          ! 进入特权配置模式
switch#set default                                     ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 4：获取 PC1 的 MAC 地址。执行“开始”→“运行”命令，在“运行”对话框的“打开”文本框中输入“cmd”命令，弹出命令行窗口，输入“ipconfig/all”命令，查看 MAC 地址，如图 4-1-9 所示。

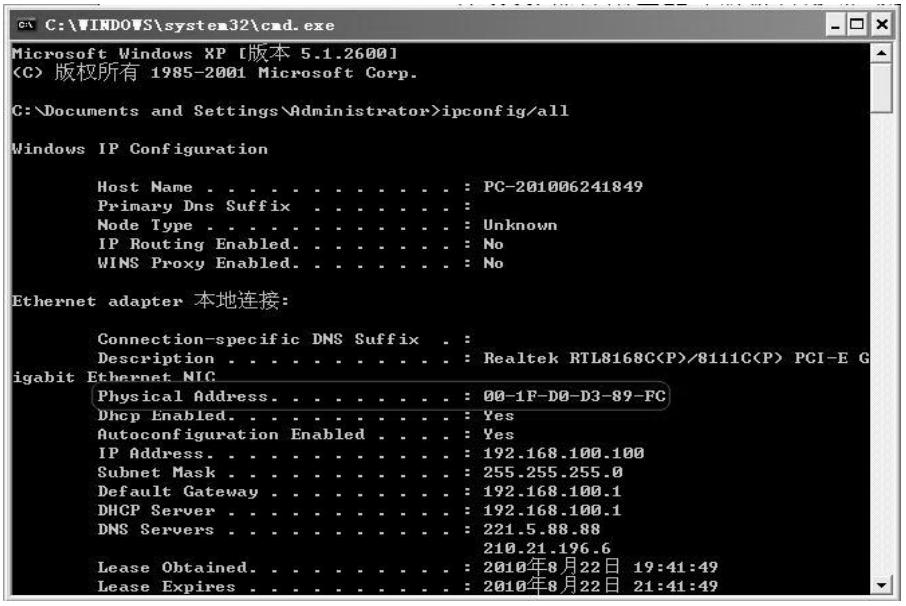

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig/all
Windows IP Configuration
Host Name . . . . . : PC-201006241849
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E G
igabit Ethernet NIC
Physical Address. . . . . : 00-1F-D0-D3-89-FC
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.100.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DHCP Server . . . . . : 192.168.100.1
DNS Servers . . . . . : 221.5.88.88
210.21.196.6
Lease Obtained. . . . . : 2010年8月22日 19:41:49
Lease Expires . . . . . : 2010年8月22日 21:41:49

图 4-1-9　查看 MAC 地址

步骤 5：配置全局 MAC-IP 命名访问列表。

```
SwitchA(config)#mac-ip-access-list extended try10
SwitchA (Config-MacIp-Ext-Nacl-try10)#permit host-source-mac 00-24-1D-B9-66-65 any-de
stination-mac ip host-source 192.168.1.100 any-destination
SwitchA (Config-MacIp-Ext-Nacl-try10)#deny any-source-mac any-destination-mac ip any-
source any-destination
```

步骤 6：查看全局 MAC-IP 命名访问列表。

```
SwitchA (config)#show access-lists
mac-ip-access-list extended try10(used 0 time(s))
   permit host-source-mac 00-24-1d-b9-66-65 any-destination-mac ip host-source
192.168.1.100 any-destination
deny any-source-mac any-destination-mac ip any-source any-destination
```

步骤 7：配置访问控制列表开启功能。

```
sw1(config)#firewall enable
sw1(config)#firewall default permit
```

步骤 8：查看访问控制列表功能开启效果。

```
SwitchA (config)#show firewall
Fire wall is enabled.
Firewall default rule is to permit any ip packet.
```

步骤 9：绑定全局 MAC-IP 命名访问列表到端口。

```
SwitchA (config)#int e0/0/1
sw1(Config-If-Ethernet0/0/1)#mac-ip access-group try10 in
```

步骤 10：查看配置。

```
SwitchA (config)#show access-group
```

```
interface name:Ethernet0/0/1
   MAC-IP Ingress access-list used is try10,traffic-statistics Disable.
No access-list configuration on VLANs!
```

步骤 11：使用 ping 命令验证连通性，见表 4-1-3。

表 4-1-3　验证表

PC	端　口	ping	结　果
PC1	0/0/1	192.168.1.1	通
PC1	0/0/10	192.168.1.1	通
PC2	0/0/1	192.168.1.1	不通
PC2	0/0/10	192.168.1.1	通

知识拓展

ARP Guard 功能：其基本原理就是利用交换机的过滤表项，检测从端口输入的所有 ARP 报文，如果 ARP 报文的源 IP 地址是受到保护的 IP 地址，则直接丢弃报文，不再转发。

举例：在端口 Ethernet0/0/1 上启动并配置 ARP Guard 地址 192.168.1.1（设为网关地址），如图 4-1-10 所示。

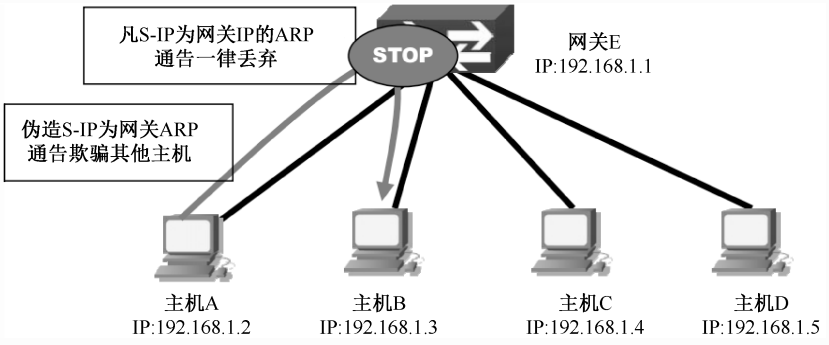


图 4-1-10　ARP Guard 功能示例图

```
Switch(Config)#interface ethernet0/0/1
Switch(Config- Ethernet 0/0/1)# arp-guard ip 192.168.1.1
```

端口 Ethernet0/0/1 端口发出的仿冒网关 ARP 报文都会被丢弃，所以 ARP Guard 功能常用于保护网关不被攻击。

ARP Guard 的优点：配置简单，适用于 ARP 仿冒网关攻击防护的快速部署。

ARP Guard 的缺点：ARP Guard 需要占用芯片 FFP 表项资源，交换机每端口配置数量有限。

学习小结

本学习活动实现了交换机的 AM 功能，可以使用将 IP 地址和 MAC 地址捆绑的方式来实现安全性的访问，将网络威胁隔离在交换机的每个端口内，而不致于对整网产生危害。

学习任务 2　IP 访问控制列表

IP ACL（IP 访问控制列表）可对流经路由器或交换机的数据包以一定的规则进行过滤，从而提高网络可管理性和安全性。其主要分为标准 IP 访问控制列表、扩展 IP 访问控制列表和基于时间的访问控制列表等。本任务分以下五个学习活动进行。

学习活动 1　标准访问控制列表的配置。
学习活动 2　扩展访问控制列表的配置。
学习活动 3　命名访问控制列表的配置。
学习活动 4　基于时间的访问控制列表。
学习活动 5　使用 ACL 过滤特定病毒报文。

学习活动 1　标准访问控制列表的配置

学习情境

某公司组建了公司内部网络，其中有财务部、技术部、市场部等部门。为了保证公司财务安全，公司经理让网络管理员禁止技术部门员工访问财务部门的主机。

情境分析

应用了 ACL 之后，交换机会在相应端口上检查某一方向的数据包，如果数据包与 ACL 的某一条规则匹配成功，则应用该规则的动作：允许该数据包通过或者丢弃该数据包。标准访问控制列表匹配规则元素只包括 IP 数据包的源 IP 地址，这意味着标准 ACL 只检查 IP 数据包的源 IP 地址。

所需设备：
（1）DCS-3950 交换机 1 台。
（2）DCRS-5650 交换机 1 台。
（3）PC 1 台。
（4）Console 线 1 条。
（5）直通双绞线 3 条。
公司内部网络拓扑结构如图 4-2-1 所示。

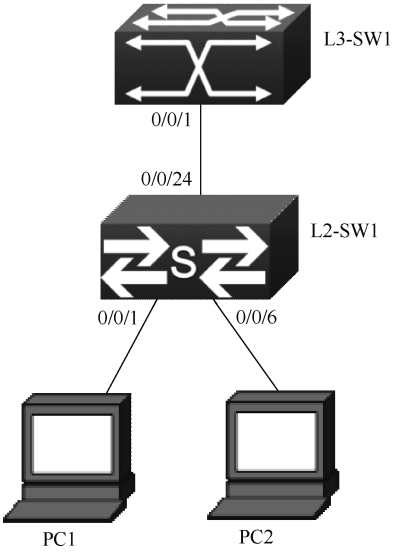


图 4-2-1　公司内部网络拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 4-2-1。

表 4-2-1　交换机和 PC 的 IP 地址网络参数设置

设　备	VLAN	端　口	IP 地址	子网掩码	网　关
L2-SW1	10	1～5			
	11	6～10			
L3-SW1	10	1～5	192.168.10.254	255.255.255.0	
	11	6～10	192.168.11.254	255.255.255.0	
PC1			192.168.10.1	255.255.255.0	192.168.10.254
PC2			192.168.11.1	255.255.255.0	192.168.11.254

相关知识

标准 IP 访问控制列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤。

IP 访问控制列表通过对数据流进行检查和过滤，来限制网络中通信数据的类型，限制网络用户以及用户所访问的设备。ACL 由一系列有序的 ACE 组成，每一个 ACE 都定义了匹配条件及行为。标准 ACL 只能针对源 IP 地址制定匹配条件，对于符合匹配条件的数据包，ACE 执行所规定的行为：允许或拒绝。

可以在设备的入站方向或者出站方向上应用 ACL。如果在设备的入站方向上应用了 ACL，设备在端口上收到数据包后，先进行 ACL 规定的检查。检查从 ACL 的第一个 ACE 开始，将 ACE 规定的条件和数据包内容进行比较和匹配。如果第一个 ACE 没有匹配成功，则匹配下一个 ACE，以此类推。一旦匹配成功，则执行该 ACE 规定的行为。如果整个 ACL 中所有的 ACE 都没有匹配成功，则执行设备定义的默认行为。被 ACL 放行的数据包则进一步执行设备的其他策略，如路由转发。

如果路由器某接口出站方向应用了 ACL，则路由器首先进行路由转发决策，发送到该接口的数据包应用 ACL 检查。检查过程与入站方向一致。

定义 ACL，应当遵循以下规则。

（1）设备接口的一个方向只能应用一个 ACL。

（2）ACL 匹配自顶向下，逐条匹配。

（3）一旦某一个 ACE 匹配成功，则立即执行该 ACE 的行为，否则停止匹配。

（4）如果所有 ACE 都没有匹配成功，则执行设备定义的默认行为。

（5）一般情况而言，在什么设备上、什么接口上、什么方向上应用 ACL，必须遵循以下约定。

① 标准 ACL 一般应用在离数据流的目的地尽可能近的地方。

② 扩展 ACL 一般应用在离数据流的源尽可能近的地方。

尽管大部分厂商推出了更高级的 ACL，但是绝大部分的网络管理员只使用两种 ACL：标准 ACL 和扩展 ACL。尽管功能比较简单，但标准 ACL 在限制 Telnet 访问路由器、限制通过 HTTP 访问设备，以及路由过滤更新方面，仍然有着较大的应用。

标准 ACL 的编号为 1～99、1300～1999。

在全局配置模式下，配置编号标准 ACL 的语法如下：

```
   access-list <num> {deny | permit} {{<sIpAddr> <sMask>} | any-source |
{host-source <sIpAddr>}}
```

该命令用于创建一条数字标准 IP 访问控制列表。如果该列表已经存在，则增加一条 ACE 表项；可以使用“ no access-list <num> ”命令来删除一条 ACL 表项。

一般情况下，配置 ACL 应遵循以下步骤。

（1）启用设备包过滤功能并配置默认行为。

（2）定义 ACL 规则。

（3）绑定 ACL 到设备接口的某一方向上。

步骤实现

步骤 1：按照图 4-2-1 连接网络拓扑结构。

步骤 2：按照表 4-2-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
switch>enable                              ! 进入特权配置模式
switch#set default                         ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                              ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 4：三层交换机的基本配置。

```
switch>enable                              ! 进入特权模式
switch#config                              ! 进入全局配置模式
switch(config)#hostname L3-SW1             ! 设置交换机名称
L3-SW1 (config)#VLAN 10                    ! 创建VLAN10
```

```
L3-SW1 (config-VLAN10)#exit                    ！退出全局配置模式
L3-SW1 (config)#VLAN 11                        ！创建VLAN11
L3-SW1 (config-VLAN11)#exit                    ！退出全局配置模式
```

步骤 5：二层交换机的基本配置。

```
switch>enable                                  ！进入特权模式
switch#config                                  ！进入全局配置模式
switch(config)#hostname L2-SW1                 ！设置交换机名称
L2-SW1 (config)#
```

步骤 6：在二层交换机上创建 VLAN、添加 VLAN 接口，并配置 Trunk 口。

```
L2-SW1 (config)#VLAN 10                        ！创建VLAN10
L2-SW1 (config-VLAN10)#switchport interface ethernet 0/0/1-5
                                               ！为VLAN10分配接口成员
L2-SW1 (config-VLAN10)#exit                    ！退出全局配置模式
L2-SW1 (config)#VLAN 11                        ！创建VLAN11
L2-SW1 (config-VLAN11)#switchport interface ethernet 0/0/6-10
                                               ！为VLAN11分配接口成员
L2-SW1 (config-VLAN11)#exit                    ！退出全局配置模式
L2-SW1 (config)#interface ethernet 0/0/24              ！进入24的接口配置模式
L2-SW1 (config-Ethernet0/0/24)#switchport mode trunk   ！设置端口为Trunk模式
Set the port Ethernet0/0/24 mode TRUNK successfully    ！成功创建Trunk口
```

步骤 7：在三层交换机上配置 VLAN、Trunk 口，并为 VLAN 指定 IP 地址。

```
L3-SW1 (config)#VLAN 10                                ！创建VLAN10
L3-SW1 (config-VLAN10)#exit                            ！退出全局配置模式
L3-SW1 (config)#VLAN 11                                ！创建VLAN11
L3-SW1 (config-VLAN11)#exit                            ！退出全局配置模式
L3-SW1 (config)#interface ethernet 0/1/1               ！进入接口配置模式
L3-SW1 (config-Ethernet1/1)#switchport mode trunk      ！设置端口为Trunk模式
Set the port Ethernet0/0/1 mode TRUNK successfully     ！成功创建Trunk口
L3-SW1 (config)#interface VLAN 10                      ！创建VLAN10的SVI
L3-SW1 (config-if-Vlan 10)#ip address 192.168.10.254 255.255.255.0
                                                       ！为VLAN10指定IP地址
L3-SW1 (config-if-Vlan 10)#no shutdown                 ！启用该SVI
L3-SW1 (config-if-Vlan 11)#exit                        ！退出全局配置模式
L3-SW1 (config)#interface VLAN 11                      ！创建VLAN11的SVI
L3-SW1 (config-if-Vlan 11)#ip address 192.168.11.254 255.255.255.0
                                                       ！为VLAN11指定IP地址
L3-SW1 (config-if-Vlan 11)#no shutdown                 ！启用该SVI接口
L3-SW1 (config-Vlan 11)#exit                           ！退出全局配置模式
```

步骤 8：验证。在 PC1 上使用 ping 命令测试 PC1 与 PC2 的连通性，如图 4-2-2 所示。

图 4-2-2　PC1 可以连通 PC2

步骤 9：在三层交换机 L3-SW1 上启用包过滤功能，设置默认行为为允许；定义 ACL 并应用。

```
L3-SW1 (config)#firewall enable                    ！开启包过滤功能
L3-SW1 (config)#firewall default permit            ！设置默认行为为允许
L3-SW1 (config)#access-list 10 deny 192.168.10.0 0.0.0.255
                                                   ！创建编号的标准ACL
L3-SW1 (config)#interface ethernet 0/1/1           ！进入1/1的接口配置模式
L3-SW1 (config-Ethernet1/1)#ip access-group 10 in
                                                   ！在接口的入站方向应用ACL
```

步骤 10：验证。在 PC1 上使用 ping 命令测试 PC1 与 PC2 的连通性。结果显示 PC1 不能再访问 PC2，即 ACL 阻断了技术部门对财务部门的访问，如图 4-2-3 所示。

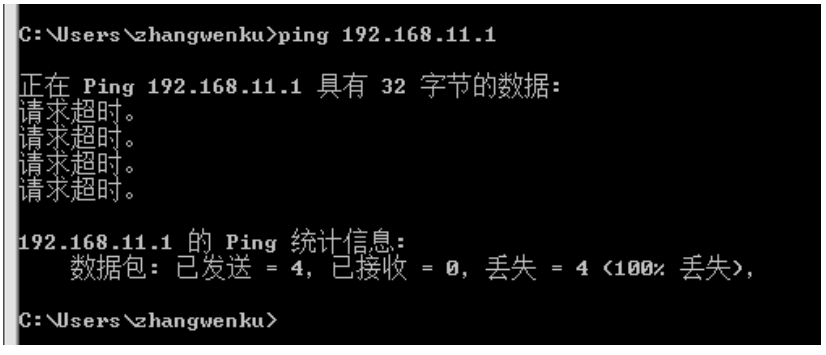


图 4-2-3　PC1 无法连通 PC2

步骤 11：在 L3-SW1 上查看配置。

```
L3-SW1 #show access-group              ！查看三层交换机ACL的应用
Interface name:Ethernet 0/1/1
   Ingress access-list used is 10.
```

小贴士

可以用编号来命名 IP 访问控制列表，也可以用名称来定义 IP 访问控制列表。如果使用编号来定义 ACL，则需要注意编号的范围。

访问控制列表总体说来有三个作用：安全控制、流量过滤、数据流量标识。

ACL 语句的顺序很重要，约束性最强的语句应该放在列表的顶部，约束性最弱的语句应

该放在列表的底部；一般而言，在一条 ACL 中不能只有允许语句，同样，也不能只有拒绝语句。虽然设备设置了默认行为，但是作为一个好习惯，在制定 ACL 时，应尽量自己定义 ACL 的最后语句。

当我们根据实际情况定义了一个 ACL，并且把它应用到相应接口的相应方向上时，就需要使用 access-group 来描述这个 ACL。access-group 是对特定的一条 access-list 与特定端口的绑定关系的描述。

知识拓展

在路由器上使用标准 ACL 实现网段的隔离。在路由器 RouterA 或者 RouterB 上创建 ACL，阻断 PC2 访问 PC1。

所需设备：

（1）DCR 2626 路由器 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）交叉线 2 条。

标准 ACL 训练拓扑结构如图 4-2-4 所示。

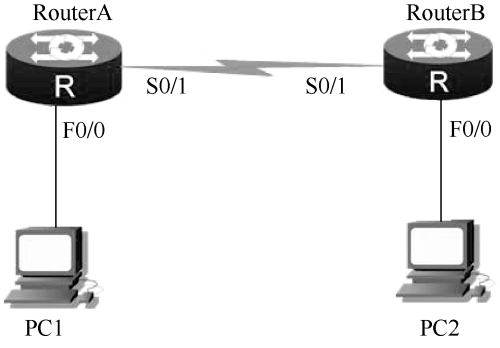


图 4-2-4　标准 ACL 训练拓扑结构

IP 地址配置表见表 4-2-2。

表 4-2-2　IP 地址配置表

设　　备	IP 地址	子网掩码
RouterA 的 F0/0 接口	192.168.1.1	255.255.255.0
RouterB 的 F0/0 接口	192.168.3.1	255.255.255.0
RouterA 的 S0/1 接口	192.168.2.1	255.255.255.0
RouterB 的 S0/1 接口	192.168.2.2	255.255.255.0
PC1	192.168.1.2	255.255.255.0
PC2	192.168.3.2	255.255.255.0

步骤 1：RouterA 的基本配置。

```
Router> enable                                    ！进入特权模式
Router#config                                     ！进入全局配置模式
Router_config#hostname routerA                    ！设置路由器名称
RouterA_config#interface fastethernet0/0          ！进入快速以太口网0/0的接口模式
RouterA_config_f0/0#ip address 192.168.1.1 255.255.255.0      ！设置IP地址
RouterA_config_f0/0#interface serial0/1           ！进入串口0/1接口模式
RouterA_config_s0/1#ip address 192.168.2.1 255.255.255.0      ！设置IP地址
RouterA_config_s0/1#no shutdown                   ！开启端口
RouterA_config_s0/1#exit                          ！退出接口模式
```

步骤 2：在 RouterA 上配置静态路由。

```
RouterA_config#ip route 192.168.3.0 255.255.255.0 192.168.2.2 ！设置静态路由
查看RouterA的静态路由表。
RouterA#show ip route                             ！查看RouterA的路由表
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      192.168.1.0/24       is directly connected, FastEthernet0/0
C      192.168.2.0/24       is directly connected, Serial0/1
S      192.168.3.0/24       [1,0] via 192.168.2.2(on Serial0/1)
```

步骤 3：RouterB 的基本配置。

```
Router>enable                                     ！进入特权模式
Router#config                                     ！进入全局配置模式
Router_config#hostname RouterB                    ！设置路由器名称
RouterB_config#interface fastethernet0/0          ！进入快速以太网0/0的接口模式
RouterB_config_f0/0#ip address 192.168.3.1 255.255.255.0      ！设置IP地址
RouterB_config_f0/0#no shutdown                   ！开启端口
RouterB_config_f0/0#interface serial0/1           ！进入串口0/1接口模式
RouterB_config_s0/1#ip address 192.168.2.2 255.255.255.0      ！设置IP地址
RouterB_config_s0/1#physical-layer speed 64000                ！设置时钟频率
RouterB_config_s0/1#no shutdown                   ！开启端口
RouterB_config_s0/1#exit                          ！退出接口模式
```

步骤 4：在 RouterB 上配置静态路由。

```
RouterB_config#ip route 192.168.1.0 255.255.255.0 192.168.2.1 ！设置静态路由
RouterB#show ip route                             ！查看RouterB的路由表
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
```

```
          DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

    VRF ID: 0

    S      192.168.1.0/24       [1,0] via 192.168.2.1(on Serial0/1)
    C      192.168.2.0/24       is directly connected, Serial0/1
    C      192.168.3.0/24       is directly connected, FastEthernet0/0
```

步骤 5：在 PC1 上测试其与 PC2 的连通性，如图 4-2-5 所示。

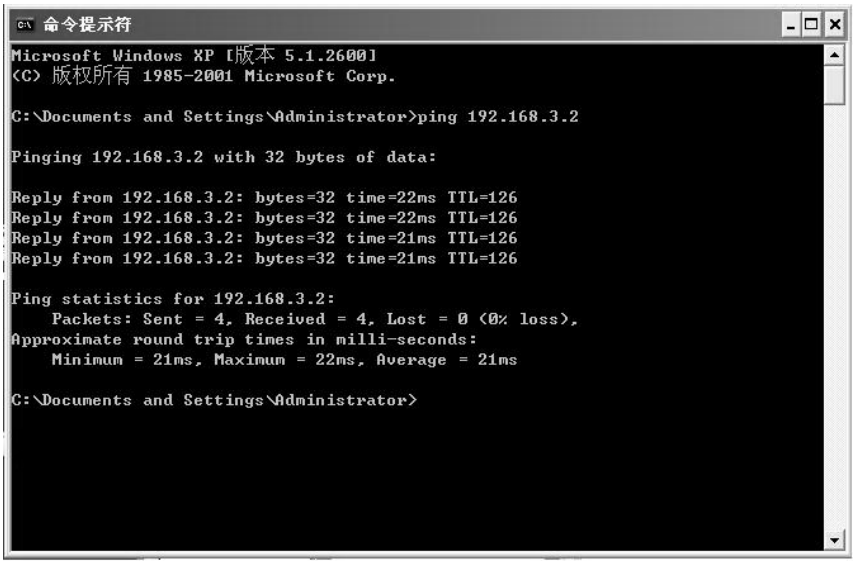

命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=22ms TTL=126
Reply from 192.168.3.2: bytes=32 time=22ms TTL=126
Reply from 192.168.3.2: bytes=32 time=21ms TTL=126
Reply from 192.168.3.2: bytes=32 time=21ms TTL=126
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 21ms, Maximum = 22ms, Average = 21ms
C:\Documents and Settings\Administrator>

图 4-2-5　测试效果（一）

步骤 6：配置禁止 PC1 连通 PC2 的命令。

```
    RouterB#config
    RouterB_config#ip acc ext denyPING
    RouterB config ext nacl#deny icmp 192.168.3.2 255.255.255.255 192.168.1.2
255.255.255.255 0
    RouterB_config_ext_nacl#permit ip any any
    RouterB config ext nacl#exit
    RouterB config#interface f0/0
    RouterB_config_f0/0#ip acc denyPING in
```

步骤 7：查看配置的 ACL。

```
    RouterB#show ip access-lists
    Extended IP access list denyPING
     deny   icmp 192.168.3.2 255.255.255.255 192.168.1.2 255.255.255.255 0
     permit ip any any
    RouterB#
```

步骤 8：验证。PC1 ping PC2 被禁止了，如图 4-2-6 所示。

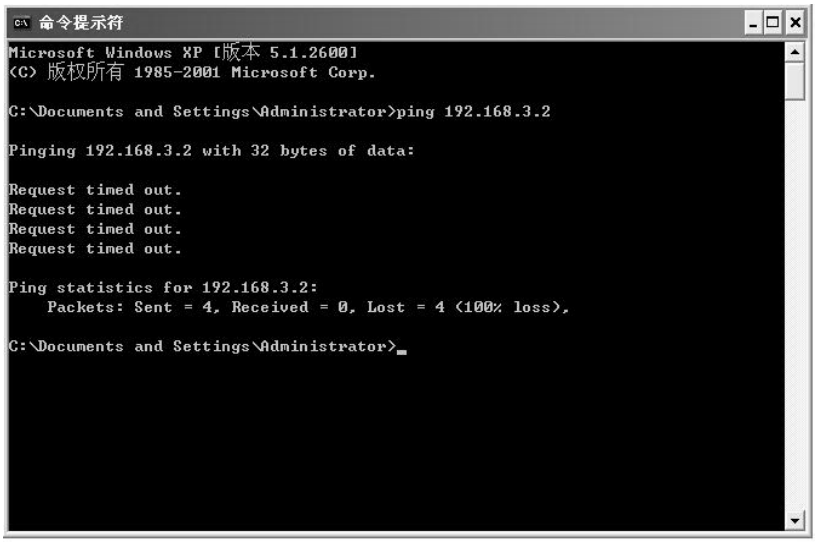


图 4-2-6　测试效果（二）

步骤 9：反之，在 PC2 上 ping PC1，可以连通，表示访问控制列表设置正确，如图 4-2-7 所示。

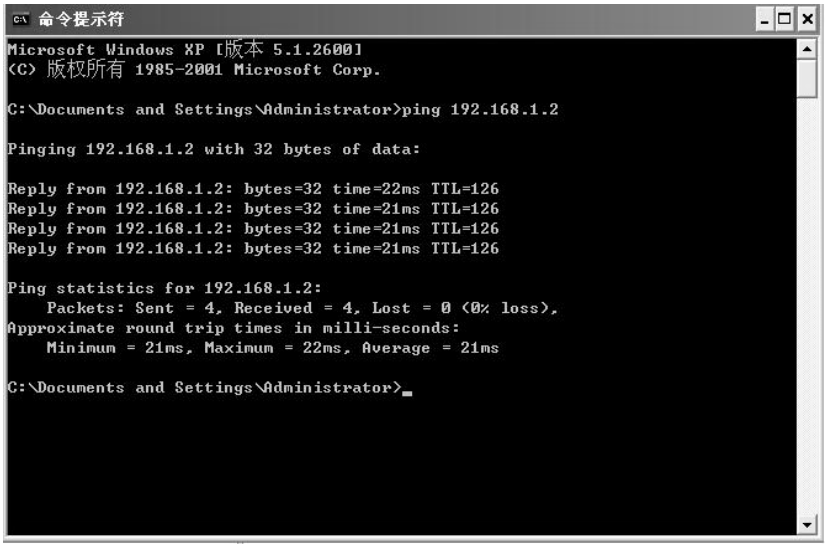


图 4-2-7　测试效果（三）

学习小结

本学习活动实现了在路由网络（三层交换机或者路由器）上使用标准 ACL 保护安全敏感网段的功能。标准 ACL 可以通过检测 IP 数据包的源 IP 地址来实现对数据包的过滤功能。标准 ACL 功能较为简单，在一些限制源 IP 地址网段的网络安全设施中应用较为广泛。

学习活动 2　扩展访问控制列表的配置

学习情境

公司为了提升工作效率，购买了专门的服务器，用于搭建公司的办公自动化系统。基于安全上的考虑，公司希望禁止销售部门的员工访问服务器的 FTP 服务，只能访问公司服务器的其他服务。

情境分析

在交换机上配置扩展 ACL，禁止 VLAN10 所属网段 192.168.10.0/24 访问 VLAN100 所属网段 192.168.100.0/24 的 TCP 端口的 20 和 21。在三层交换机上开启防火墙 ACL 检查功能，设置默认动作为 Permit，并在 Trunk 端口入站方向应用 ACL。PC1 访问 Server1 FTP 服务器的数据包将被 ACL 丢弃，其他数据包则被放行。

所需设备：

（1）DCS-3950 交换机 1 台。

（2）DCRS-5650 交换机 1 台。

（3）PC 1 台。

（4）Console 线 1 条。

（5）直通双绞线 3 条。

公司内部网络拓扑结构如图 4-2-8 所示。

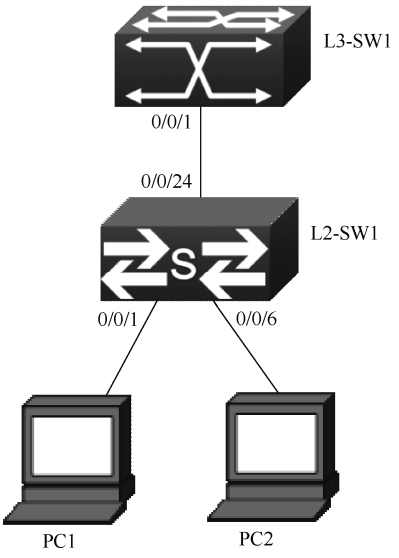


图 4-2-8　公司内部网络拓扑结构

交换机和 PC 的 IP 地址网络参数设置见表 4-2-3。

表 4-2-3　交换机和 PC 的 IP 地址网络参数设置

	VLAN	端　口	IP 地址	子网掩码	网　关
L2-SW1	10	6～10			
	100	1～5			
L3-SW1	10	6～10	192.168.10.254	255.255.255.0	
	100	1～5	192.168.100.254	255.255.255.0	
PC1			192.168.10.1	255.255.255.0	192.168.10.254
Server			192.168.100.1	255.255.255.0	192.168.100.254

相关知识

与标准 ACL 相比，扩展 ACL 所检查的数据包元素要丰富很多，它不仅可以检查数据流

的源 IP 地址，还可以检查目的 IP 地址、源端口地址和目的端口地址以及协议类型。扩展 ACL 通常用于那些精确的、高级的访问控制。FTP 服务通常使用 TCP 协议的 20 和 21 端口，使用扩展 ACL 可以精确匹配那些访问 FTP 服务的数据包并采取相应措施。

编号的扩展 ACL 的值为 100～199 和 2000～2699。

扩展 ACL 通常用在尽量靠近数据流源地址的地方。

定义扩展 ACL 的语法如下：

```
    access-list <num> {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source |
{host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination |
{host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>]
[tos <tos>][time-range<time-range-name>]
```

步骤实现

步骤 1：按照图 4-2-8 连接网络拓扑结构。

步骤 2：按照表 4-2-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：清空交换机的配置。

```
    switch>enable                                          ！进入特权配置模式
    switch#set default                                     ！恢复出厂设置
    Are you sure?[Y/N] = y
    switch#write
    switch#reload                                          ！重启交换机
    Process with reboot? [Y/N]y
```

步骤 4：三层交换机的基本配置。

```
    switch>enable                              ！进入特权模式
    switch#config                              ！进入全局配置模式
    switch(config)#hostname L3-SW1             ！设置交换机名称
    L3-SW1(config)#VLAN 10                     ！创建VLAN10
    L3-SW1(config-VLAN10)#exit                 ！退出全局配置模式
    L3-SW1(config)#VLAN 100                    ！创建VLAN100
    L3-SW1(config-VLAN100)#exit                ！退出全局配置模式
```

步骤 5：二层交换机的基本配置。

```
    switch>enable                              ！进入特权模式
    switch#config                              ！进入全局配置模式
    switch(config)#hostname L2-SW1             ！设置交换机名称
    L2-SW1(config)#
```

步骤 6：在二层交换机上创建 VLAN、添加 VLAN 接口，并配置 Trunk 口。

```
    L2-SW1(config)#VLAN 100                        ！创建VLAN100
    L2-SW1(config-VLAN100)#switchport interface ethernet 0/0/6-10
                                                   ！为VLAN100分配接口成员
    L2-SW1(config-VLAN100)#exit                    ！退出全局配置模式
    L2-SW1(config)#VLAN 10                         ！创建VLAN100
    L2-SW1(config-VLAN100)#switchport interface ethernet 0/0/6-10
                                                   ！为VLAN10分配接口成员
```

```
    L2-SW1(config-VLAN10)#exit                    ！退出全局配置模式
    L2-SW1(config)#interface ethernet 0/0/24          ！进入接口24的接口配置模式
    L2-SW1(config-Ethernet0/0/24)#switchport mode trunk   ！设置端口为Trunk模式
    Set the port Ethernet0/0/24 mode TRUNK successfully   ！成功创建Trunk口
```

步骤 7：在三层交换机上配置 VLAN、Trunk 口，并为 VLAN 指定 IP 地址。

```
    L3-SW1(config)#VLAN 10                                ！创建VLAN10
    L3-SW1(config-VLAN10)#exit                            ！退出全局配置模式
    L3-SW1(config)#VLAN 100                               ！创建VLAN100
    L3-SW1(config-VLAN100)#exit                           ！退出全局配置模式
    L3-SW1(config)#interface ethernet 1/1                 ！进入接口配置模式
    L3-SW1(config-Ethernet1/1)#switchport mode trunk      ！设置端口为Trunk模式
    Set the port Ethernet0/0/1 mode TRUNK successfully    ！成功创建Trunk口
    L3-SW1(config)#interface VLAN 10                      ！创建VLAN10的SVI
    L3-SW1(config-if-Vlan 10)#ip address 192.168.10.254 255.255.255.0
                                                          ！为VLAN10指定IP地址
    L3-SW1(config-if-Vlan 10)#no shutdown                 ！启用该SVI
    L3-SW1(config-if-Vlan 11)#exit                        ！退出全局配置模式
    L3-SW1(config)#interface VLAN 100                     ！创建VLAN100的SVI
    L3-SW1(config-if-Vlan 100)#ip address 192.168.100.254 255.255.255.0
                                                          ！为VLAN指定IP地址
    L3-SW1(config-if-Vlan 100)#no shutdown                ！启用该SVI
```

步骤 8：在三层交换机 L3-SW1 上启用包过滤功能，设置默认行为为允许；定义 ACL 并应用。

```
    L3-SW1(config)#firewall enable                        ！开启控制列表包过滤功能
    L3-SW1(config)#firewall default permit                ！设置默认动作为允许
    L3-SW1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255 192.168.100.0
0.0.0.255 d-port 20
    L3-SW1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255 192.168.100.0
0.0.0.255 d-port 21                                       ！创建编号的扩展ACL
    L3-SW1(config)#interface ethernet 1/1                 ！进入接口1/1的接口配置模式
    L3-SW1(config-Ethernet1/1)#ip access-group 100 in ！在接口的入站方向应用ACL
```

步骤 9：在 L3-SW1 上查看配置。

```
    L3-SW1#show firewall                                  ！查看防火墙配置
    Firewall Status: Enable.
    Firewall Default Rule: Permit.
    L3-SW1#show access-lists                              ！查看三层交换机ACL配置
    access-list 100(used 1 time(s)) 2 rule(s)
      access-list 100 deny tcp 10.0.0.0 0.0.0.255 192.168.100.0 0.0.0.255 d-port
d-port 20
      access-list 100 deny tcp 10.0.0.0 0.0.0.255 192.168.100.0 0.0.0.255 d-port
d-port 21
    L3-SW1#show access-group                              ！查看三层交换机ACL应用
    Interface name:Ethernet1/1
       Ingress access-list used is 100.
```

小贴士

在本例中，只需要制定目的 IP 地址的端口范围即可满足需要，在其他需求中，还需要制定源端口地址。

在端口上应用扩展 ACL 同应用标准 ACL 一样，只是扩展 ACL 检查的比较精确而已。

课堂训练

在本例所示网络拓扑中，使用扩展 ACL 实现高级的访问控制。禁止 PC1 访问 Server1 的 WWW 服务。

所需设备：

（1）DCR2626 路由器 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）交叉线 2 条。

VLAN 规划表和 IP 地址配置表见表 4-2-4 和表 4-2-5。

表 4-2-4　VLAN 规划表

设　备	端　口	VLAN ID
L2-SW1	ethernet 0/0/1-3	100
L2-SW1	ethernet 0/0/4-6	10
L3-SW1	ethernet 1/1 TRUNK	10、100

表 4-2-5　IP 地址配置表

设　备	IP 地址	网　关
L3-SW1 的 VLAN10	192.168.10.254/24	
L3-SW1 的 VLAN100	192.168.100.254/24	
PC1	192.168.10.1/24	192.168.10.254
Server1	192.168.100.1/24	192.168.100.254

学习小结

本学习活动学习了使用扩展 ACL 实现对网络访问的高级控制。扩展 ACL 可以对更多的元素进行精确匹配。定义 ACL 时，应注意数据流的方向；在接口上使用扩展 ACL 时，应尽量靠近数据流的源。此外，应当熟悉一些常见网络协议所使用的端口，如 HTTP、Web、FTP、DNS、Telnet 等。

学习活动 3　命名访问控制列表的配置

学习情境

某公司的网络工程师发现了近期网络上流行的震荡波病毒，为了防范这些病毒，网络工程师要在公司连接外网的路由器上配置命名 ACL，防范震荡波病毒侵入公司内部，危及网络安全。

情境分析

在路由器外网入站方向配置扩展 ACL，过滤外网访问内网的数据包，将病毒拒之“门”外，以维护内网的安全和稳定。

所需设备：

（1）DCR-2626 路由器 1 台。

（2）DCRS-5650 交换机 1 台。

（3）PC 1 台。

（4）交换机和路由器 Console 线各 1 条。

（5）直通双绞线 3 条。

公司连接外网示意图如图 4-2-9 所示。

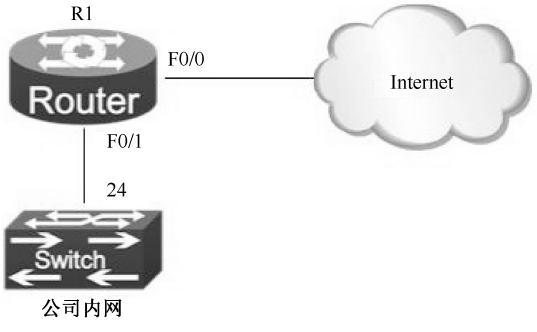


图 4-2-9　公司连接外网示意图

交换机和路由器 IP 地址网络参数设置见表 4-2-6。

表 4-2-6　交换机和路由器 IP 地址网络参数设置

设　备	端　口	VLAN ID	IP 地址	子网掩码
R1	F0/0		100.100.100.1	255.255.255.0
	F0/1		192.168.200.253	255.255.255.0
L3-SW1	0/0/24	200	192.168.200.254	255.255.255.0

相关知识

编号的访问控制列表的编号除了用于识别 ACL 的类别之外，并无其他含义。工程师往往使用很多 ACL，他们希望每个 ACL 有自己的名称，通过这些有一定意义的名称来识别它们。

标准 ACL 的编号为 1～99 和 1300～1999，扩展 ACL 的编号为 100～199 和 2000～2699。这些编号有耗尽之忧，而命名的 ACL 则无此担忧。

命名的 IP ACL 的名称可以由数字或者英文字符表示。创建命名的 ACL 时，应当使用“ ip ”命令开口。

震荡波病毒会给网络带来巨大的破坏，目前已经产生很多变种。一般情况而言，震荡波病毒通常使用 TCP 端口 445、5554 和 9996 来传播。

步骤实现

步骤 1：按照图 4-2-9 连接网络拓扑结构。

步骤 2：清空交换机的配置。

```
switch>enable                                          ！进入特权配置模式
switch#set default                                     ！恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ！重启交换机
Process with reboot? [Y/N]y
```

步骤 3：三层交换机的基本配置。

```
switch>enable                                  ！进入特权模式
switch#config                                  ！进入全局配置模式
switch(config)#hostname L3-SW1                 ！设置交换机名称
L3-SW1(config)#VLAN 200                        ！创建VLAN200
L2-SW1(config-VLAN200)#switchport interface ethernet 1/24
                                               ！为VLAN200分配接口成员
L3-SW1(config-VLAN200)#exit                    ！退出全局配置模式
L3-SW1(config)#interface VLAN 200              ！创建VLAN200的SVI
L3-SW1(config-if-Vlan 10)#ip address 192.168.200.254 255.255.255.0
                                               ！为VLAN200指定IP地址
```

步骤 4：路由器的基本配置。

```
Router>enable                                  ！进入特权模式
Router#config                                  ！进入全局配置模式
Router_config#hostname R1                      ！设置路由器名称
R1_config#interface f0/0                       ！进入f0/0的接口模式
R1_config_f0/0#ip address 100.100.100.1 255.255.255.0
                                               ！配置接口IP地址
R1_config_f0/0#no shutdown                     ！启用接口
R1_config_f0/0#exit                            ！退出全局配置模式
R1_config#interface f0/1                       ！进入f0/1的接口模式
```

```
R1_config_f0/0#ip address 192.168.200.253 255.255.255.0
                                              !配置接口IP地址
R1_config_f0/0#no shutdown                    !启用接口
R1_config_f0/0#exit                           !退出全局配置模式
```

步骤 5：在路由器上创建命名扩展 ACL，开启路由器访问控制功能，设置默认动作为全部通过，并应用 ACL 到接口。

```
R1_config#ip access-list extended Deny_virus       !创建扩展命名ACL
R1_config_ext_nacl#deny tcp any any d-port 445     !屏蔽TCP目标端口445
R1_config_ext_nacl#deny tcp any any d-port 5554    !屏蔽TCP目标端口5554
R1_config_ext_nacl#deny tcp any any d-port 9996    !屏蔽TCP目标端口9996
R1_config_ext_nacl#exit                            !退出到全局配置模式
R1_config#firewall enable                          !开启控制列表包过滤功能
R1_config#firewall default permit                  !设置默认动作为允许
R1_config#interface f0/0                           !进入f0/0的接口模式
R1_config_f0/0#ip access-group Deny_virus in       !绑定ACL到端口
```

步骤 6：在路由器上查看配置。

```
R1#show firewall                    !查看防火墙配置
Firewall Status: Enable.
Firewall Default Rule: Permit.
R1#show access-lists                !查看路由器ACL配置
Extended IP access-list Deny virus
   deny tcp any any d-port 445
   deny tcp any any d-port 5554
   deny tcp any any d-port 9996
```

小贴士

编号的 ACL 中，其编号有耗尽的可能，命名 ACL 则不会有此限制。

配置命名 ACL 时，是在 ACL 配置模式下进行的。在 ACL 配置模式下，各命令参数等同于编号的 ACL。

在接口中应用命名 ACL 时，与编号 ACL 相同，只是要将编号替换为 ACL 的名称。

课堂训练

在图 4-2-10 所示的网络拓扑中，请尝试使用命名 ACL 禁止财务部访问外网的 WWW 服务，禁止技术部访问外网的 FTP 服务。

所需设备：

（1）DCR 2600 路由器 1 台。

（2）PC 2 台。

（3）DCS-5650 三层交换机 1 台。

（4）双绞线 3 条。

命名 ACL 训练拓扑结构如图 4-2-10 所示。

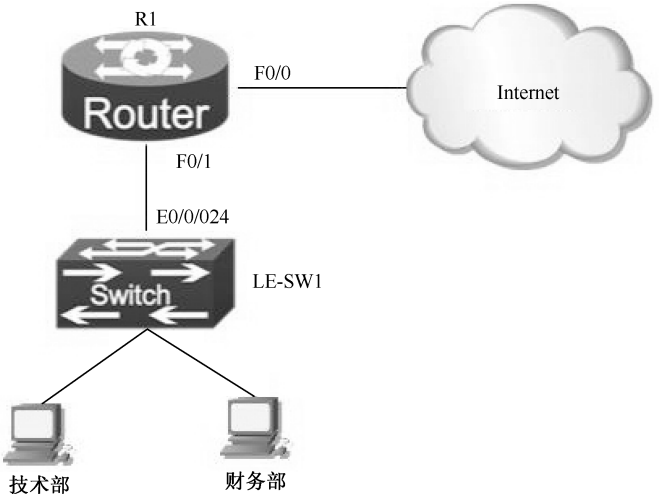


图 4-2-10　命名 ACL 训练拓扑结构

VLAN 规划表和 IP 地址配置表见表 4-2-7 和表 4-2-8。

表 4-2-7　VLAN 规划表

设　备	端　口	VLAN ID
L3-SW1	Ethernet 0/24	200
L3-SW1	Ethernet 0/1～5	10
L3-SW1	Ethernet 0/6～10	20

表 4-2-8　IP 地址配置表

设　备	IP 地址	网　关
R1 的 F0/0	100.100.100.1/24	
R1 的 F0/1	192.168.200.253/24	
L3-SW1 的 VLAN10	192.168.10.254/24	
L3-SW1 的 VLAN20	192.168.20.254/24	
L3-SW1 的 VLAN200	192.168.200.254/24	
技术部 PC	192.168.10.1/24	192.168.10.254
财务部 PC	192.168.20.1/24	192.168.20.254

学习小结

本学习活动学习了使用命名 ACL 防御外网病毒的攻击。当我们配置网络设备时，往往会创建多个 ACL。仅仅用编号来识别 ACL 的作用是比较困难的。然而，为 ACL 配置一个有意义的名称，管理员们能容易地区分这些 ACL 的作用，而不会感到困惑。

学习活动 4　基于时间的访问控制列表

学习情境

如果你是公司的网络管理员，为了保证公司员工上班时间的工作效率，公司要求 192.168.1.0 网段上班时间不能访问 IP 地址为 192.168.3.2 的 Web 服务器上的网站，下班以后访问网络不受限制。

情境分析

公司为了保证员工上班时间的工作效率，在上班时间限制员工访问某 Web 服务器网站，下班以后访问网络不受限制。这要求使用基于时间的访问控制列表来实现。

所需设备：

（1）DCR2600 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）Console 配置线 1 条。

（6）交叉线 2 条。

路由安全通信实验拓扑结构如图 4-2-11 所示。

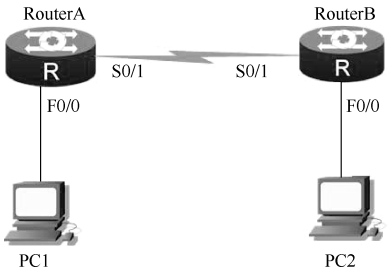


图 4-2-11　路由安全通信实验拓扑结构

IP 地址配置表见表 4-2-9。

表 4-2-9　IP 地址配置表

设　　备	IP 地址	子网掩码
RouterA 的 F0/0 接口	192.168.1.1	255.255.255.0
RouterB 的 F0/0 接口	192.168.3.1	255.255.255.0
RouterA 的 S0/1 接口	192.168.2.1	255.255.255.0
RouterB 的 S0/1 接口	192.168.2.2	255.255.255.0
PC1	192.168.1.2	255.255.255.0
PC2	192.168.3.2	255.255.255.0

相关知识

基于时间的访问控制列表是指在标准或扩展的访问控制列表的基础上增加时间段的应用规则，time-range 时间段分为两种：周期性时间段和绝对时间段。

在周期性的时间段有一些常见参数：weekdays 表示每周的工作日（周一至周五）、weekend 表示周末（周六和周日）、daily 表示每天。

在绝对时间段的表示上一般从 XXXX 年 XX 月 XX 日 XX 时 XX 分至 XXXX 年 XX 月 XX 日 XX 时 XX 分。

步骤实现

步骤 1：RouterA 的基本配置。

```
Router>enable                                          ！进入特权模式
Router#config                                          ！进入全局配置模式
Router_config#hostname RouterA                         ！设置路由器名称
RouterA_config#interface fastethernet0/0               ！进入快速以太网口0/0的接口模式
RouterA_config_f0/0#ip address 192.168.1.1 255.255.255.0      ！设置IP地址
RouterA_config_f0/0#interface serial0/1                ！进入串口0/1接口模式
RouterA_config_s0/1#ip address 192.168.2.1 255.255.255.0      ！设置IP地址
RouterA_config_s0/1#no shutdown                        ！开启端口
RouterA_config_s0/1#exit                               ！退出接口模式
```

步骤 2：在 RouterA 上配置静态路由。

```
RouterA_config#ip route 192.168.3.0 255.255.255.0 192.168.2.2 ！配置静态路由
RouterA#show ip route                                  ！查看RouterA的路由表
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C      192.168.1.0/24      is directly connected, FastEthernet0/0
C      192.168.2.0/24      is directly connected, Serial0/1
S      192.168.3.0/24      [1,0] via 192.168.2.2(on Serial0/1)
```

步骤 3：RouterB 的基本配置。

```
Router>enable                                          ！进入特权模式
Router#config                                          ！进入全局配置模式
Router_config#hostname RouterB                         ！设置路由器名称
RouterB_config#interface fastethernet0/0               ！进入快速以太口0/0接口模式
RouterB_config_f0/0#ip address 192.168.3.1 255.255.255.0      ！设置IP地址
RouterB_config_f0/0#no shutdown                        ！开启端口
RouterB_config_f0/0#interface serial0/1                ！进入串口0/1接口模式
RouterB_config_s0/1#ip address 192.168.2.2 255.255.255.0      ！设置IP地址
RouterB_config_s0/1#physical-layer speed 64000         ！设置时钟频率
RouterB_config_s0/1#no shutdown                        ！开启端口
RouterB_config_s0/1#exit                               ！退出接口模式
```

步骤 4：在 RouterB 上配置静态路由。

```
RouterB_config#ip route 192.168.1.0 255.255.255.0 192.168.2.1 ！配置静态路由
```

```
RouterB#show ip route                                    !查看RouterB的路由表
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S      192.168.1.0/24       [1,0] via 192.168.2.1(on Serial0/1)
C      192.168.2.0/24       is directly connected, Serial0/1
C      192.168.3.0/24       is directly connected, FastEthernet0/0
```

步骤 5：在 PC1 上测试其与 PC2 的连通性，如图 4-2-12 所示。

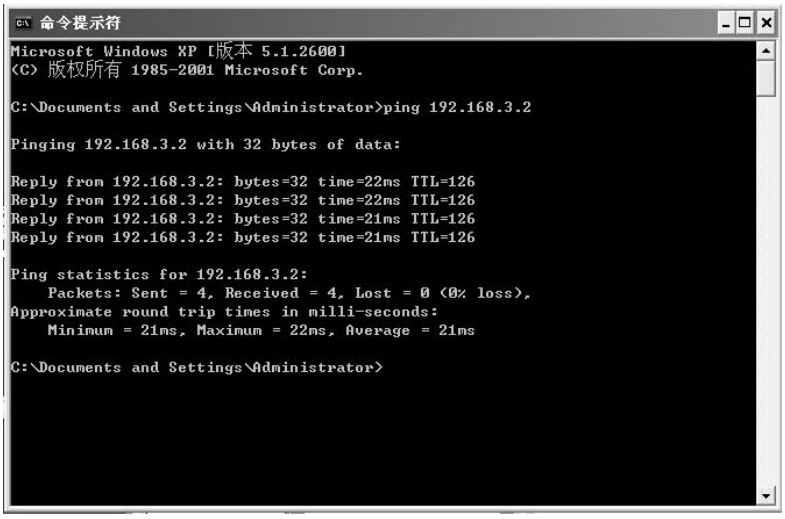

命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=22ms TTL=126
Reply from 192.168.3.2: bytes=32 time=22ms TTL=126
Reply from 192.168.3.2: bytes=32 time=21ms TTL=126
Reply from 192.168.3.2: bytes=32 time=21ms TTL=126
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 21ms, Maximum = 22ms, Average = 21ms
C:\Documents and Settings\Administrator>

图 4-2-12　测试效果

步骤 6：配置禁止访问网页的时间。

```
RouterA_config#time-range shangban                  !建立时间表shangban
RouterA_config_time_range#periodic weekdays 8:00 to 12:00     !设置周期性时间
RouterA_config_time_range#periodic weekdays 13:30 to 17:30    !设置周期性时间
RouterA_config_time_range#exit                      !退出时间表设置模式
查看time-range：
RouterA#show time-range                             !查看时间表
time-range entry: shangban (inactive)
       periodic weekdays 08:00 to 12:00
       periodic weekdays 13:30 to 17:30
RouterA#
```

步骤 7：配置基于时间的访问控制列表。

```
RouterA config#ip access-list extended denyWANGYE
!建立基于时间的访问控制列表denyWANGYE
RouterA_config_ext_nacl#deny tcp 192.168.1.0 255.255.255.0 192.168.3.2
```

```
255.255.255.255 eq 80 time-range shangban
    ！拒绝192.168.1.0网段在规定时间内访问192.168.3.2上的网页
    RouterA_config_ext_nacl#permit ip any any      ！允许所有IP数据包通过
    RouterA_config_ext_nacl#exit                   ！退出列表配置模式
    查看RouterA上的访问控制列表。
    RouterA#show ip access-lists                   ！查看访问控制列表
    Extended IP access list denyWANGYE
     deny   tcp 192.168.1.0 255.255.255.0 192.168.3.2 255.255.255.255 eq www
time-range shangban
     permit ip any any
    RouterA#
```

步骤 8：将访问控制列表绑定到相应端口。

```
    RouterA_config#interface fastethernet0/0       ！进入快速以太网口0/0的接口模式
    RouterA_config_f0/0#ip access-group denyWANGYE in
```

课堂训练

经理不允许员工在上班时间访问 QQ，但在上班时间之外可以访问，上班时间为 9:00～17:00（周一至周六），通过使用基于时间的访问控制列表来实现。PC1 模拟员工计算机，PC2 模拟外网的服务器。

所需设备：

（1）DCR2600 路由器 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）Console 配置线 1 条。

（6）交叉线 2 条。

路由安全通信实验拓扑结构如图 4-2-13 所示。

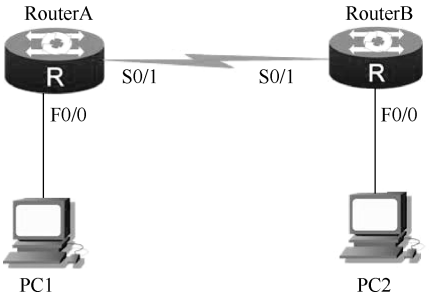


图 4-2-13　路由安全通信实验拓扑结构

IP 地址配置表见表 4-2-10。

表 4-2-10　IP 地址配置表

设　　备	IP 地址	子网掩码
RouterA 的 F0/0 接口	192.168.1.1	255.255.255.0
RouterB 的 F0/0 接口	192.168.3.1	255.255.255.0
RouterA 的 S0/1 接口	192.168.2.1	255.255.255.0
RouterB 的 S0/1 接口	192.168.2.2	255.255.255.0
PC1	192.168.1.2	255.255.255.0
PC2	192.168.3.2	255.255.255.0

学习小结

本学习活动学习了基于时间的访问控制列表。当我们配置基于时间的访问控制列表时，需要注意时间的准确性和不同专有名词的英文意义，网络管理员往往会将专业术语弄错，以致访问控制列表无法起到应有的作用。

学习活动 5　使用 ACL 过滤特定病毒报文

学习情境

某公司的网络管理员早晨上班的时候发现公司的网络不正常，经过分析之后发现是公司的计算机中了病毒，使用杀毒软件查杀证实是冲击波和震荡波的病毒，于是网络管理员想在三层交换机上通过配置 ACL 来进行隔离。

情境分析

冲击波、震荡波曾经给网络带来沉重的打击，到目前为止，整个 Internet 中还有这种病毒以及病毒的变种，它们无孔不入，伺机发作。因此在配置网络设备的时候，要采用 ACL 进行过滤，把这些病毒拒之“门”外，保证网络的稳定运行。

所需设备：

（1）DCRS-5650 交换机 1 台

（2）PC 1 台。

（3）Console 线 1 条

（4）直通网线若干。

ACL 过滤特定病毒报文拓扑结构如图 4-2-14 所示。

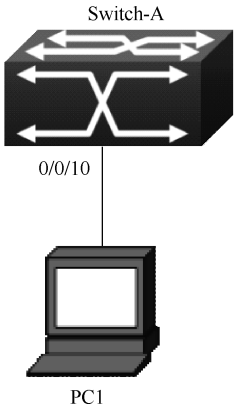


图 4-2-14　ACL 过滤特定病毒报文

相关知识

常用的端口号如下。

冲击波及冲击波变种：关闭 TCP 端口 135、139、445 和 593，关闭 UDP 端口 69（TFTP）、135、137 和 138，关闭用于远程命令外壳程序的 TCP 端口 4444。

震荡波：关闭 TCP 端口 5554、445、9996。

SQL 蠕虫病毒：关闭 TCP 端口 1433、UDP 端口 1434。

步骤实现

步骤 1：按照图 4-2-14 连接网络拓扑结构。

步骤 2：清空交换机的配置。

```
switch>enable                                          ! 进入特权配置模式
switch#set default                                     ! 恢复出厂设置
Are you sure?[Y/N] = y
switch#write
switch#reload                                          ! 重启交换机
Process with reboot? [Y/N]y
```

步骤 3：配置 ACL。

```
switch>enable
switch#config
Switch(Config)#hostname Switch-A
Switch-A(Config)#access-list 110 deny tcp any any d-port 445
Switch-A(Config)#access-list 110 deny tcp any any d-port 4444
Switch-A(Config)#access-list 110 deny tcp any any d-port 5554
Switch-A(Config)#access-list 110 deny tcp any any d-port 9996
Switch-A(Config)#access-list 110 deny tcp any any d-port 1433
Switch-A(Config)#access-list 110 deny udp any any d-port 1434
```

步骤 4：启用 ACL。

```
Switch-A(Config)#firewall enable                ! 配置访问控制列表功能开启
Switch-A(Config)#firewall default permit        ! 默认动作为全部允许通过
```

步骤 5：应用 ACL。

```
Switch-A(Config)#interface ethernet 0/0/10      ! 绑定ACL到各端口
Switch-A(Config-Ethernet0/0/10)#ip access-group 110 in
```

学习小结

本学习活动学习了如何使用 ACL 过滤特定病毒报文。在实际的工作岗位上，经常会遇到各种各样的病毒，使用 ACL 可以有效地过滤特定的病毒报文，以保证公司网络环境的稳定和安全。

学习任务 3　路由器 IPSec VPN 隧道的实现

学习情境

由于公司规模的扩大，总公司和分公司之间出于安全性的考虑，想在两个公司的出口之间使用更安全的 VPN 连接方式，网络管理员认为路由器的 IPSec VPN 可以实现此功能。

情境分析

IPSec VPN 是现在互联网上最重要的网关到网关 VPN 技术，它已经成为企业分支机构间互连的首选。总部和分支之间要实现互访时，就涉及此类 VPN，或者需要将数据包进行加密时就涉及 IPSec VPN。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）Console 线 1 条。

（6）交叉线 2 条。

IPSec VPN 网络拓扑结构如图 4-3-1 所示。

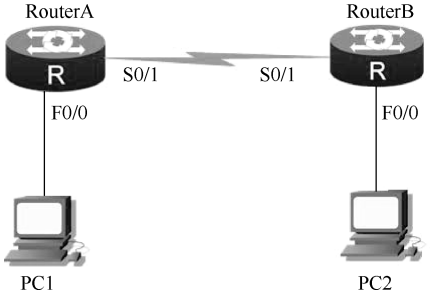


图 4-3-1　IPSec VPN 网络拓扑结构

IP 地址配置表见表 4-3-1。

表 4-3-1　IP 地址配置表

设　　备	IP 地址	子网掩码
RouterA 的 F0/0 接口	192.168.10.1	255.255.255.0
RouterB 的 F0/0 接口	192.168.20.1	255.255.255.0
RouterA 的 S0/1 接口	192.168.100.1	255.255.255.0
RouterB 的 S0/1 接口	192.168.100.2	255.255.255.0
PC1	192.168.10.2	255.255.255.0
PC2	192.168.20.2	255.255.255.0

相关知识

VPN（Virtual Private Network，虚拟专用网）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。使用这条隧道可以对数据进行几倍加密达到安全使用互联网的目的。虚拟专用网是对企业内部网的扩展。它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信

的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路；还可用于经济有效地连接到商业伙伴和用户的安全外联网虚拟专用网。VPN 可以提供的功能有防火墙功能、认证、加密、隧道化。

根据不同的划分标准，VPN 可以按以下几个标准进行分类。

1. 按 VPN 的协议分类

VPN 的隧道协议主要有三种：PPTP、L2TP 和 IPSec。其中 PPTP 和 L2TP 协议工作在 OSI 模型的第二层，又称为二层隧道协议；IPSec 是第三层隧道协议。

2. 按 VPN 的应用分类

（1）Access VPN（远程接入 VPN）：客户端到网关，使用公网作为骨干网在设备之间传输 VPN 数据流量。

（2）Intranet VPN（内联网 VPN）：网关到网关，通过公司的网络架构连接来自同公司的资源。

（3）Extranet VPN（外联网 VPN）：与合作伙伴企业网构成 Extranet，将一个公司与另一个公司的资源进行连接。

3. 按所用的设备类型分类

网络设备提供商针对不同客户的需求，开发出了不同的 VPN 网络设备，主要为交换机、路由器和防火墙。

（1）路由器式 VPN：部署较容易，只要在路由器上添加 VPN 服务即可。

（2）交换机式 VPN：主要应用于连接用户较少的 VPN 网络。

（3）防火墙式 VPN：最常见的一种 VPN 的实现方式，许多厂商提供这种配置类型。

4. 按照实现原理分类

（1）重叠 VPN：此 VPN 需要用户自己建立端结点之间的 VPN 链路，主要包括 GRE、L2TP、IPSec 等众多技术。

（2）对等 VPN：由网络运营商在主干网上完成 VPN 通道的建立，主要包括 MPLS、VPN 技术。

步骤实现

步骤 1：按照图 4-3-1 连接网络拓扑结构。

步骤 2：按照表 4-3-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
    Router>enable                                          ! 进入特权模式
    Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
    Router#delete                                          ! 删除配置文件
    this file will be erased,are you sure?(y/n)y
    Router#reboot                                          ! 重新启动
    Do you want to reboot the router(y/n)?y
    Please wait…
```

步骤 4：配置 RouterA 的名称及其接口 IP 地址。

```
Router>enable
Router#config
Router config#hostname  RouterA
RouterA_config#int fa0/0
RouterA config f0/0#ip add 192.168.10.1 255.255.255.0
RouterA config f0/0#no shut
RouterA_config_f0/0#int s0/1
RouterA config s0/1#physical-layer speed 2048000
RouterA config s0/1#no shut
RouterA_config_s0/1#Jan  1 00:02:40 Line on Interface Serial0/1, changed to
up
```

步骤 5：配置 RouterB 的名称及其接口 IP 地址。

```
Router>
Router>enable
Router#config
Router config#hostname  RouterB
RouterB_config#int fa0/0
RouterB config f0/0#ip add 192.168.20.1 255.255.255.0
RouterB config f0/0#no shut
RouterB_config_f0/0#int s0/1
RouterB config s0/1#physical-layer speed 2048000
RouterB config s0/1#ip add 192.168.100.2 255.255.255.0
RouterB_config_s0/1#no shut
RouterB_config_s0/1#^Z
```

步骤 6：查看 RouterA 的接口配置情况。

```
RouterA#show ip int brief
Interface               IP-Address     Method Protocol-Status
Async0/0                unassigned            manual down
Serial0/1               unassigned            manual up
Serial0/2               unassigned            manual down
FastEthernet0/0         192.168.10.1          manual up
FastEthernet0/3         unassigned            manual down
RouterA#
```

步骤 7：查看 RouterB 的接口配置情况。

```
RouterB#show ip int brief
Interface               IP-Address     Method Protocol-Status
Async0/0                unassigned            manual down
Serial0/1               192.168.100.2         manual up
Serial0/2               unassigned            manual down
FastEthernet0/0         192.168.20.1          manual up
FastEthernet0/3         unassigned            manual down
RouterB#
```

步骤 8：在 RouterA 上配置静态路由。

```
RouterA#config
```

```
RouterA_config#ip route 192.168.20.0 255.255.255.0 192.168.100.2
RouterA_config#
```

步骤 9：在 RouterB 上配置静态路由。

```
RouterB#config
RouterB_config#ip route 192.168.10.0 255.255.255.0 192.168.100.1
RouterB_config#
```

步骤 10：查看 RouterA 的路由表。

```
RouterA#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.100.0/24      is directly connected, Serial0/1
C     192.168.10.0/24     is directly connected, FastEthernet0/0
S     192.168.20.0/24     [1,0] via 192.168.100.2(on Serial0/1)
```

步骤 11：查看 RouterB 的路由表。

```
RouterB#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     192.168.100.0/24      is directly connected, Serial0/1
C     192.168.20.0/24     is directly connected, FastEthernet0/0
S     192.168.10.0/24     [1,0] via 192.168.1.1(on Serial0/1)
Router-B#
```

步骤 12：在 RouterA 上进行相关配置。

```
RouterA#
RouterA#config
RouterA_config#ip access-list extended 101          ！定义名为101的扩展访问列表
RouterA_config_ext_nacl#192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0    ！定义受保护数据
RouterA config ext nacl#exit
RouterA_config#crypto isakmp policy 10              ！定义ISAKMP策略，优先级为10
RouterA_config_isakmp#authentication pre-share      ！指定预共享密钥为其认证方法
RouterA_config_isakmp#hash md5                      ！指定MD5为协商的哈希算法
RouterA_config_isakmp#exit
```

```
RouterA_config#crypto isakmp key dcn 192.168.100.2
！配置预共享密钥为dcn的远端IP地址为192.168.100.2
RouterA_config#crypto ipsec transform-set hello   ！定义名称为hello的变换集
RouterA_config_crypto_trans#transform-type esp-des esp-md5-hmac
！设置变换类型为esp-des esp-md5-hmac
RouterA config crypto trans#exit
RouterA_config#crypto map my 10 ipsec-isakmp
！创建一个名为my序号为10指定通信为ipsec-isakmp的加密映射表
RouterA config crypto map#set peer 192.168.100.2
！在加密映射表中指定IPSec对端
RouterA config crypto map#match address 101
！为加密映射表指定一个扩展访问控制列表
RouterA_config_crypto_map#set transform-set  hello
！指定加密映射表使用的变换集合
RouterA config crypto map#exit
RouterA_config#int s0/1
RouterA_config_s0/1#crypto map my      ！将预先定义好的加密映射表集合运用到接口上
RouterA_config_s0/1#
```

步骤 13：在 RouterB 上进行相关配置。

```
RouterB#
RouterB#config
RouterB_config#ip access-list extended 101        ！定义名为101的扩展访问列表
RouterB_config_ext_nacl#192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0                                     ！定义受保护数据
RouterB config ext nacl#exit
RouterB_config#crypto isakmp policy 10            ！定义ISAKMP策略，优先级为10
RouterB_config_isakmp#authentication pre-share    ！指定预共享密钥为认证方法
RouterB_config_isakmp#hash md5                    ！指定MD5为协商的哈希算法
RouterB_config_isakmp#exit
RouterB config#crypto isakmp key dcn 192.168.100.1
！配置预共享密钥为dcn的远端IP地址为192.168.100.1
RouterB_config#crypto ipsec transform-set hello   ！定义名称为hello的变换集
RouterB config crypto trans#transform-type esp-des esp-md5-hmac
！设置变换类型为esp-des esp-md5-hmac
RouterB_config_crypto_trans#exit
RouterB config#crypto map my 10 ipsec-isakmp
！创建一个名为my、序号为10、指定通信为ipsec-isakmp的加密映射表
RouterB_config_crypto_map#set transform-set hello
！指定加密映射表使用的变换集合
RouterB config crypto map#set peer 192.168.100.1
！在加密映射表中指定IPSec对端
RouterB config crypto map#match address 101
！为加密映射表指定一个扩展访问控制列表
RouterB_config_crypto_map#exit
```

```
RouterB_config#int s0/1
RouterB_config_s0/1#crypto map my    ！将预先定义好的加密映射表集合运用到接口上
RouterB_config_s0/1#
```

小贴士

变换集合可以指定一个或两个 IPSec 安全协议（或 ESP，或 AH，或两者都有），并且指定和选定的安全协议一起使用哪种算法。如果想要提供数据机密性，则可以使用 ESP 加密变换。如果想要提供对外部 IP 报头以及数据的验证，则可以使用 AH 变换。如果使用 ESP 加密变换，则可以考虑使用 ESP 验证变换或 AH 变换来提供变换集合的验证服务。如果想要数据验证功能（或使用 ESP 或使用 AH），则可以选择 MD5 或 SHA 验证算法。SHA 算法比 MD5 健壮，但速度慢。

在执行了 crypto ipsec transform-set 命令以后，将进入加密变换配置状态。在这种状态下，可以将模式改变为隧道模式或传输模式（目前神州数码路由器只支持 tunnel 模式）。在做完这些改变以后，键入“exit”命令可返回全局配置状态。

步骤 14：查看 IPSec 的安全联盟，此时显示的信息为空信息。

```
RouterA#show crypto isakmp sa
```

步骤 15：在 PC1 上 ping 192.168.20.2，网络已连通，如图 4-3-2 所示。

图 4-3-2　连通性测试效果图

步骤 16：查看路由器 A 和路由器 B 的 IPSec 的安全联盟，此时已经触发 IPSec 形成。

```
RouterA#show crypto isakmp sa
     dst             src             state          state-id      conn
192.168.100.2  192.168.100.1  <R>Q SA SETUP        2         2 my 10
192.168.100.2  192.168.100.1  <R>M_SA_SETUP        1         2 my 10
RouterA#

RouterB#show crypto isakmp sa
     dst             src             state          state-id      conn
192.168.100.1  192.168.100.2  <I>Q SA SETUP        3         2 my 10
192.168.100.1  192.168.100.2  <I>M_SA_SETUP        2         2 my 10
RouterB#
```

小贴士

注意 IPSec 的隧道建立需要触发条件，没有数据包流量时，是不会建立 SA（安全联盟）的，所以要通过 ping 命令来产生流量。

步骤 17：查询 VPN 的策略信息。

```
RouterA#show crypto isakmp policy
Protection suite of priority 10
    encryption algorithm:    DES  - Data Encryption Standard (56 bit keys).
    hash algorithm:          Message Digest 5
    authentication method:   Pre-Shared Key
    Diffie-Hellman group:    #1 (768 bit)
    lifetime:               86400 seconds
Default protection suite
    encryption algorithm:    DES  - Data Encryption Standard (56 bit keys).
    hash algorithm:          Secure Hash Standard
    authentication method:   Pre-Shared Key
    Diffie-Hellman group:    #1 (768 bit)
    lifetime:               86400 seconds
RouterA#
RouterB#show crypto isakmp policy
Protection suite of priority 10
    encryption algorithm:    DES  - Data Encryption Standard (56 bit keys).
    hash algorithm:          Message Digest 5
    authentication method:   Pre-Shared Key
    Diffie-Hellman group:    #1 (768 bit)
    lifetime:               86400 seconds
Default protection suite
    encryption algorithm:    DES  - Data Encryption Standard (56 bit keys).
    hash algorithm:          Secure Hash Standard
    authentication method:   Pre-Shared Key
    Diffie-Hellman group:    #1 (768 bit)
    lifetime:               86400 seconds
RouterB#
```

学习小结

本学习活动介绍了路由器的 IPSec VPN 技术，这种技术是一套具有比较完整的体系的 VPN 技术，它规定了一系列的协议标准，在学习时要注意的是，VPN 技术是在网络正常通信的基础上采用的安全技术，所以在实现时，要先保证网络是连通的。

项目考核

1．实现二层交换机 DCS-3950 的 AM 功能，实验拓扑结构如图 4-3-3 所示。

2．采用 2 台 DCR2626 路由器、1 台 DCS-5650 交换机和 4 台 PC 来组建实验环境。用一台路由器（RTA）模拟整个园区网，用另一台路由器（RTB）模拟外部网。具体实验环境如图 4-3-4 所示。

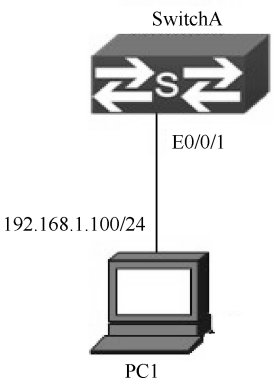


图 4-3-3　AM 功能

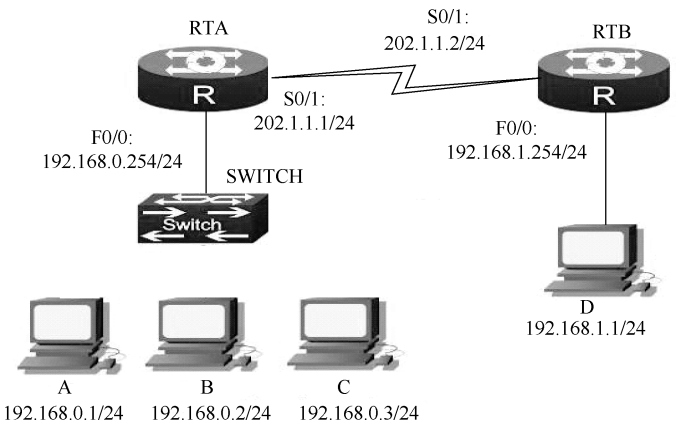


图 4-3-4　实验拓扑

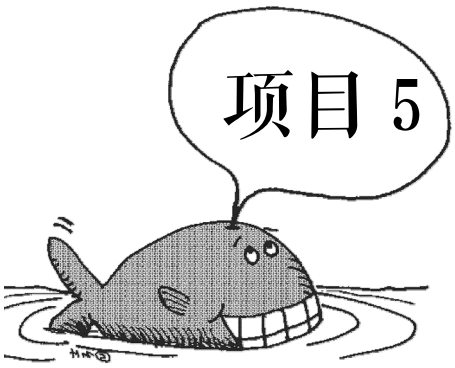
在企业的日常工作中，经常会碰到对企业内部的网络制定各种各样的访问控制，以下几条需求就模拟了现实中常见的实例。

（1）禁止 C 访问外网（即不能访问 D）。

（2）禁止 B 在 8:00～17:00 访问外网（即不能访问 D）。

（3）禁止 C 使用 Telnet 登录到路由器 RTA。

（4）禁止 D 访问 192.168.0.0 网段（可以认为主机 D 为危险对象）。



广域网协议配置

项目学习说明

广域网（Wide Area Network，WAN）也称远程网，是一种运行地域超过局域网的数据通信网络，通常跨接很大的物理范围，所覆盖的范围从几十千米到几千千米，它能连接多个城市或国家，或者横跨几个大洲并能提供远距离通信，形成国际性的远程网络。广域网和局域网的主要区别之一是需要向外部的广域网服务提供商申请订购广域网电信网络服务。一般使用电信运营商提供的数据链路在广域网范围内访问网络。

本项目重点学习路由器广域网协议的封装配置、广域网 PPP 封装验证和网络地址协议转换协议配置。

学习能力目标

学习任务 1 路由器广域网协议的封装配置
学习任务 2 路由器的广域网 PPP 封装验证
学习任务 3 网络地址转换协议（NAT）配置

职业能力目标

- 能理解广域网协议的类型与工作原理
- 能实现广域网封装协议的配置
- 能理解 PPP 中 PAP 和 CHAP 的区别
- 能实现 PPP 中 PAP 和 CHAP 的配置方法
- 能熟练理解 NAT 的工作原理
- 能熟练实现 PAT 的配置

学习任务 1　路由器广域网协议的封装配置

路由器常用的广域网协议有 PPP、HDLC 和 Fram-Relay 等。其中，PPP 是点对点协议，是面向字符的控制协议；HDLC 是高级数据链路控制协议，是面向位的控制协议；Fram-Relay 表示帧中继交换网，它是 X.25 分组交换网的改进，以虚电路的方式工作。本学习任务分成以下两个学习活动进行。

学习活动 1　路由器的广域网 HDLC 封装。

学习活动 2　路由器的广域网 PPP 封装。

学习活动 1　路由器广域网 HDLC 封装配置

点到点连接、专用链路和交换电路的默认封装类型为高级数据链路控制（High-Level Data Link Control，HDLC），HDLC 现在是同步 PPP 的基础。

学习情境

HDLC 是一个在同步网上传输数据、面向比特的数据链路层协议，它是由国际标准化组织（ISO）根据 IBM 公司的 SDLC（Synchronous Data Link Control）协议扩展开发而成的。网络管理员想在公司通过路由器来模拟公网实现 HDLC 协议的配置。

情境分析

路由器在进行广域网 HDLC 协议的封装时，需要使用广域网接口来实现，分别对两台路由器的广域网端口 S0 封装 HDLC，分配 IP 地址，并且配置静态路由，这样就可以实现公司间的通信了。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。

（4）交叉线 1 条。

（5）PC 1 台。

（6）Console 配置线 1 条。

HDLC 封装配置拓扑结构如图 5-1-1 所示。

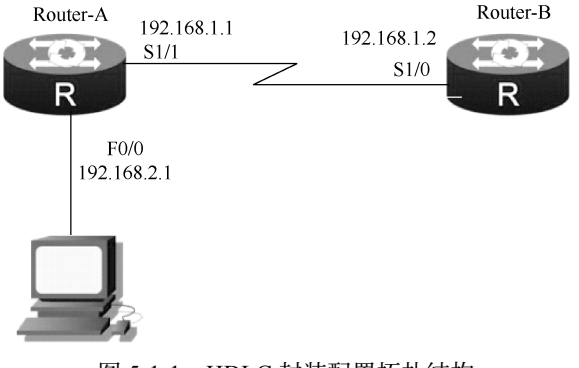


图 5-1-1　HDLC 封装配置拓扑结构

相关知识

路由器在进行广域网协议的封装时，要注意 DCE 和 DTE 端的区别，所以先了解一下 DCE

和 DTE 的概念。

DTE：数据终端设备，如终端，是广义的概念，PC 也可以是终端。一般广域网常用的 DTE 设备有路由器、终端主机。

DCE：数据通信设备，如 Modem，连接 DTE 设备的通信设备。一般广域网常用的 DCE 设备有 CSU/DSU、广域网交换机、Modem。

DTE 和 DCE 的区别：DCE 提供时钟，DTE 不提供时钟，但它依靠 DCE 提供的时钟工作，如计算机和 Modem 之间。数据传输通常先经过 DTE-DCE，再经过 DCE-DTE 的路径。其实，对于标准的串行端口，通常从外观就能判断是 DTE 还是 DCE。DTE 是针头（俗称公头），DCE 是孔头（俗称母头），这样两种接口才能接在一起。

但是，对于一个大型的网络来说，一个网络设备是接在 DCE 端还是接在 DTE 端是相对而言的，也就是说，一个设备有可能是 DCE 协议。

步骤实现

步骤 1：按照图 5-1-1 连接网络拓扑结构。

步骤 2：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0, level = 15
Router#delete                                          ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 3：Router-A 的配置。

```
Router>enable                                  ！进入特权模式
Router #config                                 ！进入全局配置模式
Router_config#hostname Router-A                ！修改机器名称
Router-A_config#interface s1/1                 ！进入接口模式
Router-A_config_s1/0#ip address 192.168.1.1 255.255.255.0     ！配置IP地址
Router-A_config_s1/1#encapsulation hdlc                ！封装HDLC协议
Router-A_config_s1/0#physical-layer speed 64000    ！配置DCE时钟频率
Router-A config s1/0#no shutdown
Router-A_config_s1/0#^Z                        ！按【Ctrl+Z】组合键进入特权模式
```

步骤 4：查看 Router-A 的配置。

```
Router-A#show interface s1/1                       ！查看接口状态
Serial1/0 is up, line protocol is down             ！对端没有配置，所以协议是down
Mode=Sync DCE Speed=64000                          ！查看DCE
DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP
Interface address is 192.168.1.1/24                ！查看IP地址
MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
Encapsulation protocol HDLC, link check interval is 10 sec ！查看封装协议
```

```
Octets Received0, Octets Sent 0
Frames Received 0, Frames Sent 0, Link-check Frames Received0
Link-check Frames Sent 89, LoopBack times 0
Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0
Link-check Timeout 0, Queue Error 0, Link Error 0,
60 second input rate 0 bits/sec, 0 packets/sec!
60 second output rate 0 bits/sec, 0 packets/sec!
0 packets input, 0 bytes, 8 unused rx, 0 no buffer
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
8 packets output, 192 bytes, 0 unused_tx, 0 underruns
error:
0 clock, 0 grace
PowerQUICC SCC specific errors:
0 recv allocb mblk fail 0 recv no buffer
0 transmitter queue full 0 transmitter hwqueue full
Router-A#
```

步骤 5：Router-B 的配置。

```
Router>enable                                          ！进入特权模式
Router#config                                          ！进入全局配置模式
Router_config#hostname Router-B                        ！修改机器名
Router-B_config#interface s1/0                         ！进入接口模式
Router-B_config_s1/0#ip address 192.168.1.2 255.255.255.0     ！配置IP地址
Router-B_config_s1/1#encapsulation hdlc                ！封装HDLC协议
Router-B_config_s1/0#no shutdown
Router-B_config_s1/0#^Z                              ！按【Ctrl+Z】组合键进入特权模式
```

步骤 6：查看 Router-B 的配置。

```
Router-B#show interface s1/0                           ！查看接口状态
Serial1/0 is up, line protocol is up                   ！接口和协议都是up
Mode=Sync DTE                                          ！查看DTE
DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP
Interface address is 192.168.1.2/24                    ！查看IP地址
MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
Encapsulation protocol HDLC, link check interval is 10 sec ！查看封装协议
Octets Received0, Octets Sent 0
Frames Received 0, Frames Sent 0, Link-check Frames Received0
Link-check Frames Sent 89, LoopBack times 0
Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0
Link-check Timeout 0, Queue Error 0, Link Error 0,
60 second input rate 0 bits/sec, 0 packets/sec!
60 second output rate 0 bits/sec, 0 packets/sec!
0 packets input, 0 bytes, 8 unused_rx, 0 no buffer
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
8 packets output, 192 bytes, 0 unused tx, 0 underruns
error:
```

```
0 clock, 0 grace
PowerQUICC SCC specific errors:
0 recv allocb mblk fail 0 recv no buffer
0 transmitter queue full 0 transmitter hwqueue_full
Router-B#
```

步骤 7：在 Router-A 上配置默认路由。

```
Router-A_config#ip route 0.0.0.0 0.0.0.0 192.168.1.2
Router-A_config#
```

步骤 8：在 Router-B 上配置默认路由。

```
Router-B config#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Router-B_config#
```

步骤 9：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S      0.0.0.0/0          [1,0] via 192.168.1.2(on Serial0/1)
C      192.168.1.0/24      is directly connected, Serial0/1
C      192.168.2.0/24      is directly connected, FastEthernet0/0
Router-A#
```

步骤 10：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S      0.0.0.0/0          [1,0] via 192.168.1.1(on Serial0/1)
C      192.168.1.0/24      is directly connected, Serial0/1
Router-B#
```

步骤 11：测试连通性，如图 5-1-2 所示。

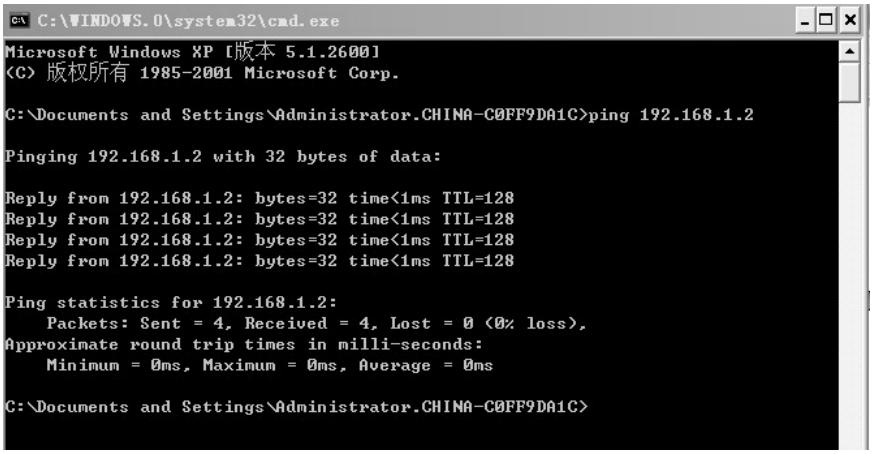


图 5-1-2　连通性测试效果图

小贴士

（1）注意查看接口状态，接口和协议都必须是 up。

（2）CR-V35FC 所连接的接口为 DCE，CR-V35MT 所连接的接口为 DTE。

（3）协议是 down，通常是因为封装不匹配、DCE 时钟没有配置。

（4）接口是 down，通常是因为线缆出现了故障。

（5）在实际工作中，DCE 设备通常由服务提供商配置，本学习活动是模拟环境。

学习小结

本学习活动实现了广域网链路中的 HDLC 协议封装的配置。路由器封装广域网协议时，必须具有相应的广域网功能模块。路由器两端封装的协议必须一致，否则无法建立链路。

学习活动 2　路由器广域网 PPP 封装配置

PPP 是一种比 HDLC 功能更加丰富、更加安全的广域网封装协议，支持身份认证、多链路捆绑等功能。

学习情境

某公司下属有多个分公司，并且总公司与分公司分别设在不同城市，为了顺利开展业务，要求总公司与分公司之间的网络通过路由器相连，并保持网络通畅。要求网络管理员在路由器上适当配置，实现公司网内部主机之间的相互通信。

情境分析

网络管理员准备通过广域网接口 S0 连接总公司与分公司。分别对两台路由器的广域网端口 S0 封装 PPP，分配 IP 地址，并且配置静态路由，设置好后即可开始通信。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。

（4）Console 线 1 条。

（5）交叉线 1 条。

（6）PC 2 台。

PPP 封装拓扑结构如图 5-1-3 所示。

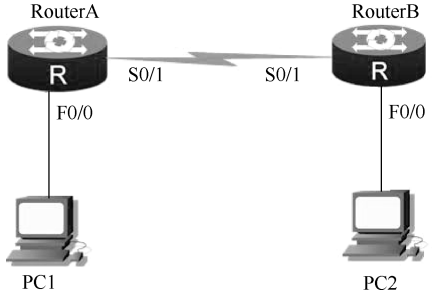


图 5-1-3　PPP 封装拓扑结构

IP 地址配置表见表 5-1-1。

表 5-1-1　IP 地址配置表

设　　备	IP 地址	子网掩码	网　　关
RouterA 的 F0/0 接口	192.168.2.1	255.255.255.0	
RouterB 的 F0/0 接口	192.168.3.1	255.255.255.0	
RouterA 的 S0/1 接口	192.168.1.1	255.255.255.0	
RouterB 的 S0/1 接口	192.168.1.2	255.255.255.0	
PC1	192.168.2.2	255.255.255.0	192.168.2.1
PC2	192.168.3.2	255.255.255.0	192.168.3.1

相关知识

PPP 协议位于 OSI 模型的数据链路层，PPP 协议按照功能划分为两个子层：LCP、NCP。LCP 主要负责链路的协商、建立、回拨、认证、数据的压缩、多链路捆绑等功能。NCP 主要负责和上层的协议进行协商，为网络层协议提供服务。

PPP 的认证功能是指在建立 PPP 链路的过程中进行密码的验证，验证通过则建立连接，验证不通过则拆除连接。

PPP 应用范围：PPP 是一种多协议成帧机制，它适合在调制解调器、HDLC 位序列线路、SONET 和其他物理层上使用。它支持错误检测、选项协商、头部压缩以及使用 HDLC 类型帧格式（可选）的可靠传输。

PPP 提供了以下三类功能。

（1）成帧：可以毫无歧义地分割出每帧的起始和结束。

（2）链路控制：LCP 支持同步和异步线路，也支持面向字节的和面向位的编码方式，可用于启动路线、测试线路、协商参数、关闭线路。

（3）网络控制：具有协商网络层选项的方法，并且协商方法与使用的网络层协议独立。

PPP 工作流程：当用户拨号接入 ISP 时，路由器的调制解调器对拨号做出确认，并建立一条物理连接。PC 向路由器发送一系列的 LCP 分组（封装成多个 PPP 帧）。这些分组及其响应选择一些 PPP 参数，进行网络层配置，NCP 给新接入的 PC 分配一个临时的 IP 地址，使 PC 成为因特网中的一个主机。通信完毕时，NCP 释放网络层连接，收回原来分配的 IP 地址，LCP 释放数据链路层连接，最后释放物理层的连接。

步骤实现

步骤 1：按照图 5-1-3 连接网络拓扑结构。

步骤 2：按照表 5-1-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                          ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                          ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…..
```

步骤 4：设置 RouterA 的主机名称和端口配置。

```
Router>enable                                                ！进入特权模式
Router #config                                               ！进入全局配置模式
Router _config#hostname RouterA                              ！修改机器名称
RouterA_config#interface s0/1                                ！进入接口模式
RouterA_config_s0/1#ip address 192.168.1.1 255.255.255.0    ！配置IP地址
RouterA_config_s0/1#encapsulation PPP                        ！封装PPP协议
RouterA_config_s0/1#physical-layer speed 64000               ！配置DCE时钟频率
RouterA config s0/1#no shutdown
RouterA config s0/1#int fa0/0
RouterA_config_f0/0#ip add 192.168.2.1 255.255.255.0
RouterA config f0/0#no shutdown
RouterA config f0/0#^Z
RouterA#
```

步骤 5：查看 RouterA 的接口配置信息。

```
RouterA#show interface s1/1                          ! 查看接口状态
Serial1/0 is up, line protocol is down               !对端没有配置, 所以协议是down
Mode=Sync DCE Speed=64000                            ! 查看DCE
DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP
Interface address is 192.168.1.1/24                  ! 查看IP地址
MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
Encapsulation protocol PPP, link check interval is 10 sec     ! 查看封装协议
Octets Received0, Octets Sent 0
Frames Received 0, Frames Sent 0, Link-check Frames Received0
Link-check Frames Sent 89, LoopBack times 0
Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0
Link-check Timeout 0, Queue Error 0, Link Error 0,
60 second input rate 0 bits/sec, 0 packets/sec!
60 second output rate 0 bits/sec, 0 packets/sec!
0 packets input, 0 bytes, 8 unused rx, 0 no buffer
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
8 packets output, 192 bytes, 0 unused tx, 0 underruns
error:
0 clock, 0 grace
PowerQUICC SCC specific errors:
0 recv allocb mblk fail 0 recv no buffer
0 transmitter queue full 0 transmitter hwqueue_full
```

步骤 6：设置 RouterB 的主机名称和端口配置。

```
Router>enable                                        ! 进入特权模式
Router#config                                        ! 进入全局配置模式
Router_config#hostname RouterB                       ! 修改机器名称
RouterB_config#interface s0/1                        ! 进入接口模式
RouterB_config_s0/1#ip address 192.168.1.2 255.255.255.0      ! 配置IP地址
RouterB_config_s0/1#encapsulation PPP                ! 封装PPP协议
RouterB_config_s0/1#no shutdown
RouterB config s0/1#int fa0/0
RouterB config f0/0#ip add 192.168.3.1 255.255.255.0
RouterB_config_f0/0#no shutdown
RouterB config f0/0#^Z
RouterB#
```

步骤 7：查看 RouterB 的接口配置信息。

```
RouterA#show interface s0/1                          ! 查看接口状态
Serial0/1 is up, line protocol is up                 ! 接口和协议都是up
Mode=Sync DTE                                        ! 查看DTE
DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP
Interface address is 192.168.1.2/24                  ! 查看IP地址
MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
Encapsulation protocol PPP, link check interval is 10 sec     ! 查看封装协议
Octets Received0, Octets Sent 0
```

```
Frames Received 0, Frames Sent 0, Link-check Frames Received0
Link-check Frames Sent 89, LoopBack times 0
Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0
Link-check Timeout 0, Queue Error 0, Link Error 0,
60 second input rate 0 bits/sec, 0 packets/sec!
60 second output rate 0 bits/sec, 0 packets/sec!
0 packets input, 0 bytes, 8 unused_rx, 0 no buffer
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
8 packets output, 192 bytes, 0 unused tx, 0 underruns
error:
0 clock, 0 grace
PowerQUICC SCC specific errors:
0 recv allocb mblk fail 0 recv no buffer
0 transmitter queue full 0 transmitter hwqueue full
RouterA#
```

步骤 8：查看 RouterA 的接口情况。

```
RouterA#show ip int brief
Interface               IP-Address      Method      Protocol-Status
Async0/0                unassigned      manual          down
Serial0/1               192.168.1.1     manual          up
Serial0/2               unassigned      manual          down
FastEthernet0/0          192.168.2.1    manual          up
FastEthernet0/3          unassigned     manual          down
RouterA#
```

步骤 9：查看 RouterB 的接口情况。

```
RouterB#show ip int brief
Interface               IP-Address      Method      Protocol-Status
Async0/0                unassigned      manual          down
Serial0/1               192.168.1.2     manual          up
Serial0/2               unassigned      manual          down
FastEthernet0/0          192.168.3.1    manual          up
FastEthernet0/3          unassigned     manual          down
RouterB#
```

步骤 10：在 RouterA 上配置默认路由。

```
RouterA config#ip route 0.0.0.0 0.0.0.0 192.168.1.2
RouterA_config#
```

步骤 11：在 RouterB 上配置默认路由。

```
RouterB config#ip route 0.0.0.0 0.0.0.0 192.168.1.1
RouterB_config#
```

步骤 12：查看 RouterA 的路由表。

```
RouterA#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
```

```
      OE1 - OSPF external type 1, OE2 - OSPF external type 2
      DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S     0.0.0.0/0          [1,0] via 192.168.1.2(on Serial0/1)
C     192.168.1.0/24      is directly connected, Serial0/1
C     192.168.1.2/32      is directly connected, Serial0/1
！32位掩码表示PPP封装
C     192.168.2.0/24      is directly connected, FastEthernet0/0
RouterA#
```

步骤 13：查看 RouterB 的路由表。

```
RouterB#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
      D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
      ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
      OE1 - OSPF external type 1, OE2 - OSPF external type 2
      DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

S     0.0.0.0/0          [1,0] via 192.168.1.1(on Serial0/1)
C     192.168.1.0/24      is directly connected, Serial0/1
C     192.168.1.1/32      is directly connected, Serial0/1
！32位掩码表示PPP封装
C     192.168.3.0/24      is directly connected, FastEthernet0/0
RouterB#
```

步骤 14：测试连通性，如图 5-1-4 所示。

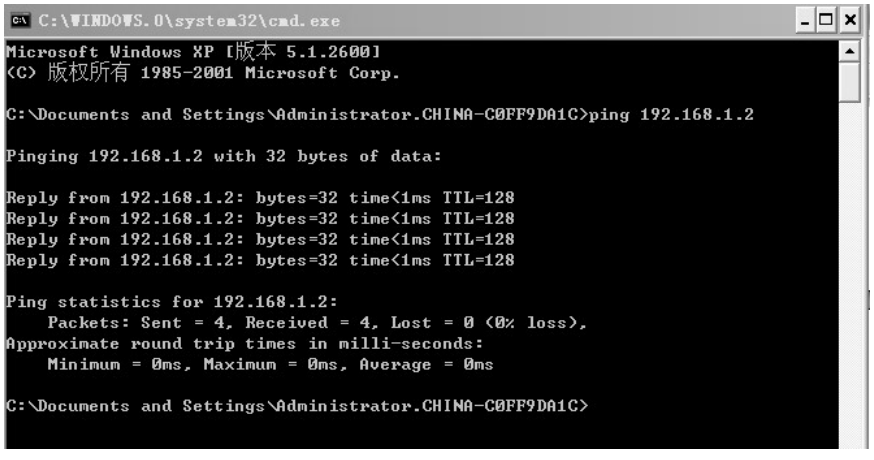

C:\WINDOWS.0\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator.CHINA-C0FF9DA1C>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator.CHINA-C0FF9DA1C>

图 5-1-4　连通性测试效果图

小贴士

注意查看接口状态，接口和协议都必须是 up。

学习小结

本学习活动实现了广域网链路中的 PPP 协议封装的配置。路由器封装广域网协议时，必须具有相应的广域网功能模块，分辨出线缆的 DCE 和 DTE。路由器两端封装的协议必须一致，否则无法建立链路。

学习任务 2　路由器广域网协议的 PPP 封装验证

广域网协议的 PPP 具有 PAP 和 CHAP 两种验证协议，PAP 认证只在链路建立初期进行，只有两次信息的交换，因此被称为两次握手。CHAP 验证比 PAP 验证安全。本学习任务分成以下两个学习活动进行。

学习活动 1　使用 PPP 的 PAP 认证。

学习活动 2　使用 PPP 的 CHAP 认证。

学习活动 1　使用 PPP 的 PAP 认证

学习情境

某公司为了满足不断增长的业务需求，申请了专线接入。公司的路由器与 ISP 进行链路协商时，需要验证身份。配置路由器以保证链路的建立，并考虑其安全性。

情境分析

WAN 专线链路建立时要进行安全认证，以保证链路的安全性。链路协商时，密码验证协议（Password Authentication Protocol，PAP）在设备之间传输用户名、密码，以实现用户身份的认证确认。公司计划在路由器上配置 PPP PAP 认证，以实现链路的安全连接。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。

（4）Console 线 1 条。

公司网络拓扑结构如图 5-2-1 所示。

图 5-2-1　公司网络拓扑结构

相关知识

PPP 支持两种认证方式 PAP 和 CHAP。PAP 是指验证双方通过两次握手完成验证过程，它是一种用于对试图登录到点对点协议服务器上的用户进行身份验证的方法。由被验证方主动发出验证请求，发送的验证包含用户名和密码。由验证方验证后做出回复，即通过验证或验证失败。在验证过程中用户名和密码以明文的方式在链路上传输。

PAP 是一种简单的明文验证方式。NAS（Network Access Server，网络接入服务器）要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接，获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 将无法提供避免受到第三方攻击的保障措施。

步骤实现

步骤 1：按照图 5-2-1 连接网络拓扑结构。

步骤 2：恢复路由器的出厂配置。

```
    Router>enable                                          ! 进入特权模式
    Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
    Router#delete                                          ! 删除配置文件
    this file will be erased,are you sure?(y/n)y
    Router#reboot                                          ! 重新启动
    Do you want to reboot the router(y/n)?y
    Please wait…..
```

步骤 3：RouterA 的基本配置。

```
    router>enable                                          ! 进入特权模式
    router#config                                          ! 进入全局配置模式
    router_config#hostname RouterA                         ! 设置路由器名称
    RouterA_config#username RouterB password digitalb      ! 设置用户名和密码
    RouterA_config#interface serial 0/1                    ! 进入串口0/1接口模式
    RouterA_config_s0/1#ip address10.0.0.1 255.255.255.0   ! 设置IP地址
    RouterA_config_s0/1#physical-layer speed 64000         ! 设置时钟频率
    RouterA_config_s0/1#no shutdown                        ! 开启端口
```

步骤 4：RouterB 的基本配置。

```
    Router>enable                                          ! 进入特权模式
    Router#config                                          ! 进入全局配置模式
    Router_config#hostname RouterB                         ! 设置路由器名称
```

```
RouterB_config#username RouterA password digitala      ！设置用户名和密码
RouterB_config#interface s0/2                          ！进入串口0/1接口模式
RouterB_config_s0/2#ip address 10.0.0.2 255.255.255.0 ！设置IP地址
RouterB_config_s0/2#no shutdown                        ！开启端口
```

步骤 5：测试 RouterA 与 RouterB 的连通性。

```
RouterB# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
!!!!!
---10.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 20/20/20 ms
RouterB#
```

步骤 6：在 RouterA 上配置 PAP 验证。

```
RouterA_config#interface s0/1                  ！进入串口0/1接口模式
RouterA_config_s0/1#encapsulation ppp          ！封装点对点协议
RouterA_config_s0/1#ppp authentication pap     ！设置认证方式为PAP
RouterA config s0/1#ppp pap sent-username RouterA password digitala
                                               ！发送认证时使用的用户名和密码
RouterA config#aaa authentication ppp default local
                                               ！设置PPP认证方式为本地用户认证
RouterA_config_s0/1#no shutdown                ！开启端口
```

步骤 7：在 RouterB 上配置 PAP 验证。

```
RouterB_config#interface s0/2                  ！进入串口0/2接口模式
RouterB_config_s0/2#encapsulation ppp          ！封装点对点协议
RouterB_config_s0/2#ppp authentication pap     ！设置认证方式为PAP
RouterB config s0/2#ppp pap sent-username RouterB password digitalb
                                               ！发送认证时使用的用户名和密码
RouterB_config#aaa authentication ppp default local
                                               ！设置PPP认证方式为本地用户认证
```

步骤 8：查看 RouterB 的接口信息。

```
RouterB#show ip interface brief                ！查看接口信息
Interface               IP-Address     Method Protocol-Status
Async0/0                unassigned     manual down
Serial0/1               unassigned     manual down
Serial0/2               10.0.0.2        manual up
FastEthernet0/0          unassigned     manual up
FastEthernet0/3          unassigned     manual down
```

步骤 9：在 RouterA 上查看 S 接口的配置。

```
RouterA#show interface s0/1                    ！查看路由器A的s0/1的信息
Serial0/1 is up, line protocol is up
 Mode=Sync  Speed=64000
  DTR=UP,DSR=UP,RTS=UP,CTS=UP,DCD=UP
  MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
  Interface address is 10.0.0.1/24
```

```
  Encapsulation PPP, loopback not set
  Keepalive set(10 sec)
  LCP  Opened
  PAP  Opened,  Message: 'Welcome to Digitalchina Router'
  IPCP Opened
      local IP address: 10.0.0.1  remote IP address: 10.0.0.2
  60 second input rate 44 bits/sec, 0 packets/sec!
  60 second output rate 44 bits/sec, 0 packets/sec!
    7342 packets input, 176838 bytes, 4 unused rx, 0 no buffer
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    7272 packets output, 105690 bytes, 8 unused tx, 0 underruns
  error:
    0 clock, 0 grace
  PowerQUICC SCC specific errors:
    0 recv allocb mblk fail     0 recv no buffer
    0 transmitter queue full    0 transmitter hwqueue_full
```

步骤 10：在 RouterB 上查看 S 接口的配置。

```
RouterB#show interface s0/2           !查看路由器B s0/2的信息
Serial0/2 is up, line protocol is up
 Mode=Sync DTE
  DTR=UP,DSR=UP,RTS=UP,CTS=UP,DCD=UP
  MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
  Interface address is 10.0.0.2/24
  Encapsulation PPP, loopback not set
  Keepalive set(10 sec)
  LCP  Opened
  PAP  Opened,  Message: 'Welcome to Digitalchina Router'
  IPCP Opened
      local IP address: 10.0.0.2  remote IP address: 10.0.0.1
  60 second input rate 34 bits/sec, 0 packets/sec!
  60 second output rate 38 bits/sec, 0 packets/sec!
    20 packets input, 504 bytes, 6 unused rx, 0 no buffer
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    21 packets output, 528 bytes, 8 unused tx, 0 underruns
  error:
    0 clock, 0 grace
  PowerQUICC SCC specific errors:
    0 recv allocb mblk fail     0 recv no buffer
0 transmitter queue full    0 transmitter hwqueue_full
```

步骤 11：测试 RouterA 与 RouterB 的连通性。

```
RouterA#ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2): 56 data bytes
!!!!!
```

```
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 20/22/30 ms
```

小贴士

PAP 通过两次握手机制，为建立远程结点的验证提供了一个简单的方法。

路由器的接口默认为关闭状态，必须使用命令将接口启动。对于串行链路，DCE 需要提供时钟信号。上述内容配置完毕后，使用 ping 命令检验两个路由器之间的链路能否正常通信。

链路两端的用户名和密码一定要保持一致，否则会导致链路认证失败。

广域网链路的两端封装的协议必须一致，否则无法建立正确的连接。

课堂训练

使用 PAP 认证方式实现路由器安全通信。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）Console 线 1 条。

（6）交叉线 2 条。

PAP 验证方式训练拓扑结构如图 5-2-2 所示。

IP 地址配置表见表 5-2-1。

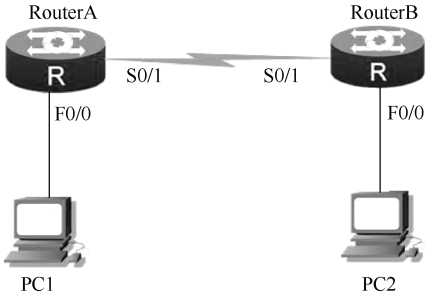


图 5-2-2　PAP 验证方式训练拓扑结构

表 5-2-1　IP 地址配置表

设　　备	IP 地址	子网掩码
RouterA 的 F0/0 接口	192.168.1.1	255.255.255.0
RouterB 的 F0/0 接口	192.168.3.1	255.255.255.0
RouterA 的 S0/1 接口	192.168.2.1	255.255.255.0
RouterB 的 S0/1 接口	192.168.2.2	255.255.255.0
PC1	192.168.1.2	255.255.255.0
PC2	192.168.3.2	255.255.255.0

学习小结

本学习任务实现了广域网链路中的 PPP 的 PAP 安全认证。PAP 是一种简单的身份认证，适用于对安全性要求不是很高的网络环境，其原理和工作过程比较简单。配置时需要注意两端用户名和密码必须保持一致。PAP 本身并不是一种很安全的认证方式，其明文传输方式有一定的安全隐患。

学习活动 2　使用 PPP 的 CHAP 认证

学习情境

考虑到增强 WAN 链路的安全功能，公司计划在路由器上配置 PPP 的 CHAP 认证，以满足日益增长的安全需求。

情境分析

CHAP（Challenge Hand Authentication Protocol，挑战握手后验证协议）使用三次握手机制来启动一条链路和周期性地验证远程结点。与 PAP 认证比较起来，CHAP 认证更具有安全性。CHAP 只在网络中传送用户名而不传送口令，因此安全性更高。

所需设备：

（1）DCR-2655 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。

（4）Console 线 1 条。

PPP CHAP 认证链接拓扑结构如图 5-2-3 所示。

图 5-2-3　PPP CHAP 认证链接拓扑结构

相关知识

CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令，其中包括会话 ID 和一个任意生成的挑战字串。远程客户必须使用 MD5 单向哈希算法返回用户名和加密的挑战口令、会话 ID 及用户口令，其中用户名以非哈希方式发送。

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字串来防止受到再现攻击。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，从而避免第三方冒充远程客户进行攻击。

步骤实现

步骤 1：按照图 5-2-3 连接网络拓扑结构。

步骤 2：恢复路由器的出厂配置。

```
Router>enable                                                    ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
Router#delete                                                    ！删除配置文件
this file will be erased,are you sure?(y/n)y
Router#reboot                                                    ！重新启动
Do you want to reboot the router(y/n)?y
Please wait…
```

步骤 3：RouterA 的基本配置。

```
Router>enable                                                    ！进入特权模式
Router#config                                                    ！进入全局配置模式
Router_config#hostname RouterA                                   ！设置路由器名称
RouterA_config#username RouterB password digital                 ！设置用户名和密码
RouterA_config#aaa authentication ppp default local
！设置PPP认证方式为本地用户认证
RouterA_config#interface s0/1                                    ！进入串口0/1接口模式
RouterA_config_s0/1#ip address 10.0.0.1 255.255.255.0              ！设置IP地址
RouterA_config_s0/1#physical-layer speed 64000                     ！设置时钟频率
RouterA_config_s0/1#no shutdown                                    ！开启端口
```

步骤 4：RouterB 的基本配置。

```
Router>enable                                                    ！进入特权模式
Router#config                                                    ！进入全局配置模式
Router_config#hostname RouterB                                   ！设置路由器名称
RouterB_config#username RouterA password digital                 ！设置用户名和密码
RouterB config#aaa authentication ppp default local
！设置PPP认证方式为本地用户认证
RouterB_config#interface s0/2                                    ！进入串口0/2接口模式
RouterB_config_s0/2#ip address 10.0.0.2 255.255.255.0              ！设置IP地址
RouterB_config_s0/2#no shutdown                                    ！开启端口
```

步骤 5：查看 RouterA 的接口信息。

```
RouterA#show ip interface brief            ！查看路由器A的接口信息
Interface               IP-Address      Method Protocol-Status
Async0/0                unassigned      manual down
Serial0/1               10.0.0.1         manual up
Serial0/2               unassigned      manual down
FastEthernet0/0         unassigned      manual down
FastEthernet0/3         unassigned      manual down
```

步骤 6：测试 RouterA 与 RouterB 的连通性。

```
RouterB#ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
!!!!!
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

```
round-trip min/avg/max = 20/22/30 ms
```

步骤 7：在 RouterA 上配置 CHAP 验证。

```
RouterA_config#interface s0/1                          ！进入串口0/1接口模式
RouterA_config_s0/1#encapsulation ppp                  ！封装点对点协议
RouterA_config_s0/1#ppp authentication chap            ！设置认证方式为CHAP
RouterA_config_s0/1#ppp chap hostname RouterA          ！设置发送给对方的用户名
RouterA_config_s0/1#ppp chap password digital          ！设置发送给对方的密码
```

步骤 8：查看 RouterA 的接口信息。

```
RouterA#show ip interface brief
Interface               IP-Address      Method Protocol-Status
Async0/0                unassigned      manual down
Serial0/1               10.0.0.1        manual down    ！已经为down
Serial0/2               unassigned      manual down
FastEthernet0/0         unassigned      manual down
FastEthernet0/3         unassigned      manual down
```

步骤 9：查看 RouterA 的串口信息。

```
RouterA#show interface s0/1                ！查看路由器A的s0/1接口信息
Serial0/1 is up, line protocol is down
 Mode=Sync DCE Speed=64000
  DTR=UP,DSR=UP,RTS=UP,CTS=UP,DCD=UP
  MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
  Interface address is 10.0.0.1/24
  Encapsulation PPP, loopback not set
  Keepalive set(10 sec)
  LCP  Opened
  CHAP Listening -- waiting for remote host to attempt open,    Message: 'CHAP:
Invalid Response'
  IPCP Listening -- waiting for remote host to attempt open
       local IP address: 10.0.0.1  remote IP address: 0.0.0.0
  60 second input rate 0 bits/sec, 0 packets/sec!
  60 second output rate 0 bits/sec, 0 packets/sec!
    71 packets input, 1878 bytes, 3 unused rx, 0 no buffer
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    67 packets output, 1766 bytes, 8 unused_tx, 0 underruns
  error:
    0 clock, 0 grace
  PowerQUICC SCC specific errors:
    0 recv allocb mblk fail     0 recv no buffer
0 transmitter queue full    0 transmitter hwqueue full
RouterA#Jan  1 00:19:06 Line on Interface Serial0/1, changed state to down
Jan  1 00:19:07 Line on Interface Serial0/1, changed state to up
Jan  1 00:19:16 Line on Interface Serial0/1, changed state to down
Jan  1 00:19:16 Line on Interface Serial0/1, changed state to up
```

步骤 10：在 RouterB 上配置 CHAP 验证。

```
RouterB_config#interface s0/2                          ！进入串口0/2接口模式
RouterB_config_s0/2#encapsulation ppp                  ！封装点对点协议
RouterB_config_s0/2#ppp authentication chap            ！设置认证方式为CHAP
RouterB_config_s0/2#ppp chap hostname RouterB          ！设置发送给对方的用户名
RouterB_config_s0/2#ppp chap password digital          ！设置发送给对方的密码
```

步骤 11：查看 RouterB 的串口信息。

```
RouterB#show interface s0/2                            ！查看RouterB的s0/2接口信息
Serial0/2 is up, line protocol is up                   ！已经变为up
 Mode=Sync DCE Speed=64000
  DTR=UP,DSR=UP,RTS=UP,CTS=UP,DCD=UP
  MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
  Interface address is 10.0.0.1/24
  Encapsulation PPP, loopback not set
  Keepalive set(10 sec)
  LCP  Opened
  CHAP Opened,  Message: ' Welcome to Digitalchina Router'    ！表示认证成功
  IPCP Opened
      local IP address: 10.0.0.1  remote IP address: 10.0.0.2
  60 second input rate 44 bits/sec, 0 packets/sec!
  60 second output rate 44 bits/sec, 0 packets/sec!
    27 packets input, 701 bytes, 5 unused_rx, 0 no buffer
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    28 packets output, 726 bytes, 8 unused tx, 0 underruns
  error:
    0 clock, 0 grace
  PowerQUICC SCC specific errors:
    0 recv allocb mblk fail     0 recv no buffer
0 transmitter queue full    0 transmitter hwqueue_full
```

步骤 12：查看 RouterA 的路由表。

```
RouterA#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     10.0.0.0/24         is directly connected, Serial0/1
C     10.0.0.2/32         is directly connected, Serial0/1 ！表示PPP已经成功
routerA#
```

步骤 13：查看 RouterB 的路由表。

```
RouterB#show  ip  route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
```

```
       D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2

VRF ID: 0

C     10.0.0.0/24         is directly connected,Serial0/2
C     10.0.0.1/32         is directly connected, Serial0/2 ！表示PPP已经成功
routerB#
```

步骤 14：测试 RouterA 与 RouterB 的连通性。

```
RouterB#ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
!!!!!
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 20/22/30 ms
```

课堂训练

使用 CHAP 认证方式实现路由器的安全通信。

所需设备：

（1）DCR 2600 路由器 2 台。

（2）PC 2 台。

（3）CR-V35MT 1 条。

（4）CR-V35FC 1 条。

（5）Console 线 1 条。

（6）交叉线 2 条。

CHAP 验证方式实验拓扑结构如图 5-2-4 所示。

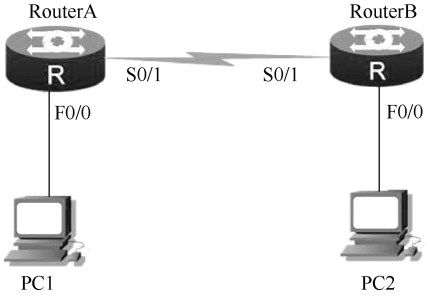


图 5-2-4　CHAP 验证方式实验拓扑结构

IP 地址配置表见表 5-2-2。

表 5-2-2　IP 地址配置表

设　　备	IP 地址	子网掩码
RouterA 的 F0/0 接口	192.168.1.1	255.255.255.0
RouterB 的 F0/0 接口	192.168.3.1	255.255.255.0
RouterA 的 S0/1 接口	192.168.2.1	255.255.255.0
RouterB 的 S0/1 接口	192.168.2.2	255.255.255.0
PC1	192.168.1.2	255.255.255.0
PC2	192.168.3.2	255.255.255.0

学习小结

本学习任务实现了广域网链路中的 PPP CHAP 安全认证。在 Internet 中传输信息时，CHAP 表现出了足够强大的抗攻击能力，可以适用于对安全性要求比较高的网络环境。在验证过程中，链路上传递的信息都进行了加密处理。配置时需要注意两端的密钥要保持一致。

学习任务 3　网络地址转换协议配置

NAT（Network Address Translation，网络地址转换）的功能是将企业内部自行定义的私有 IP 地址转换为 Internet 公网上可识别的合法 IP 地址。由于现行 IP 地址标准 —— IPv4 的限制，Internet 面临着 IP 地址空间短缺的问题，从 ISP 申请并给企业的每位员工分配一个合法 IP 地址是不现实的。NAT 技术能较好地解决现阶段 IPv4 地址短缺的问题。本学习任务分成以下两个学习活动进行。

学习活动 1　利用 NAT 实现外网主机访问内网服务器。

学习活动 2　利用动态 NAT 实现局域网访问互联网。

学习活动 1　利用 NAT 实现外网主机访问内网服务器

学习情境

某公司计划通过互联网向外发布公司的 Web 主页。目前公司已经申请了公网 IP 地址，并创建了公司内部的 Web 服务器。现在，公司希望外网用户能够像内网用户一样访问公司的 Web 服务器。

情境分析

公司为 Web 服务器申请了一个公网 IP 地址的做法是非常正确的，通过静态 NAT 的方式

可以达到公司想要的效果。

静态 NAPT（Network Address Port Frans lation，网络端口地址转换）将内部私有地址和端口号转换为内部公网地址和端口号。当外部主机访问内部公网地址时，NAT 设备将数据包中的目的 IP 地址（公网地址）与端口号转换为内部私有地址和端口号，从而实现使用公网地址向互联网发布内部服务器的目的。

所需设备：

（1）DCR-2626 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。

（4）Console 线 1 条。

（5）交叉线 2 条。

NAT 实现外网主机访问内网服务器拓扑结构如图 5-3-1 所示。

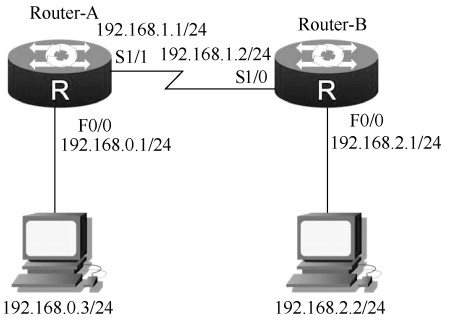


图 5-3-1　NAT 实现外网主机访问内网服务器拓扑结构

IP 地址配置表见表 5-3-1。

表 5-3-1　IP 地址配置表

设　备	IP 地址	网　关
Router-A 的 S1/1	192.168.1.1/24	
Router-A 的 F0/0	192.168.0.1/24	
Router-B 的 S1/0	192.168.1.2/24	
Router-B 的 F0/0	192.168.2.1/24	
Web Server	192.168.2.2/24	192.168.2.1
Client	192.168.0.3/24	192.168.0.1

步骤实现

步骤 1：按照图 5-3-1 连接网络拓扑结构。

步骤 2：按照表 5-3-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
    Router>enable                                          ！进入特权模式
    Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
level = 15
    Router#delete                                          ！删除配置文件
    this file will be erased,are you sure?(y/n)y
    Router#reboot                                          ！重新启动
    Do you want to reboot the router(y/n)?y
    Please wait…
```

步骤 4：Router-A 的基本配置。

```
    Router-A_config#interface fastEthernet 0/0
    Router-A_config_f0/0#ip address 192.168.0.1 255.255.255.0
```

```
Router-A_config_f0/0#no shutdown
Router-A config#interface serial 0/1
Router-A config s0/1#ip address 192.168.1.1 255.255.255.0
Router-A_config_s0/1#no shutdown
Router-A_config_s0/1#physical-layer speed 64000
```

步骤 5：Router-B 的基本配置。

```
Router-B_config#interface fastEthernet 0/0
Router-B config f0/0#ip address 192.168.2.1 255.255.255.0
Router-B config f0/0#no shutdown
Router-B_config#interface serial 0/2
Router-B config s0/2#ip address 192.168.1.2 255.255.255.0
Router-B_config_s0/2#no shutdown
```

步骤 6：配置 Router-A 的 NAT。

```
Router-A_config#ip nat inside source static 192.168.0.3 192.168.1.1
```

步骤 7：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
OE1 - OSPF external type 1, OE2 - OSPF external type 2
DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2
VRF ID: 0
C     192.168.1.0/24      is directly connected, Serial0/2
C     192.168.2.0/24      is directly connected, FastEthernet0/0
```

步骤 8：查看地址转换表。

```
Router-A#show ip nat tr
translations   -- Translation entries
Router-A#show ip nat translations
Pro. Dir Inside local    Inside global    Outside local    Outside global
---- --- 192.168.0.3     192.168.1.1       ---        ---
```

步骤 9：测试网络连通情况，如图 5-3-2 所示。

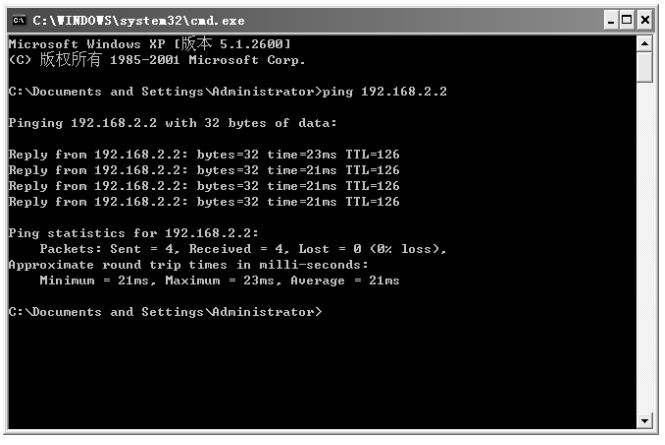

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=23ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 21ms, Maximum = 23ms, Average = 21ms
C:\Documents and Settings\Administrator>

图 5-3-2　测试效果图

小贴士

利用 NAT 技术发布内网服务器时，需要注意每种应用服务通常有自己的默认端口，这意味着我们使用一个公网 IP 地址可以发布多种内网服务。但是，对于任意一种网络服务，只能有一台内部主机成为被发布的服务器。也就是说，在只有一个公网 IP 地址的情况下，只能有一台 FTP 服务器、E-mail 服务器、WWW 服务器可以发布到网络中。

解决这个问题其实并不难，如内网中有 2 台 Web 服务器，可以使用公网地址的 TCP 端口 80 来发布第 1 台 Web 服务器，使用 TCP 端口 8000 来发布第 2 台 Web 服务器。但是，客户机访问第 2 台服务器时，需要添加上端口地址，如“http://100.100.100.1:8000”，才可以正确访问。

课堂训练

在 R1 路由器上配置静态 NAPT，利用 R1 的公网 IP 地址（202.96.0.1）发布内网服务器 FTP Server 的 FTP 服务（TCP 端口 20、21）。使得右侧内部主机 Client 可以通过公网地址（FTP://202.96.0.1）访问左侧的 FTP 服务器。

所需设备：

（1）DCR-2600 路由器 2 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）双绞线 3 条。

发布 FTP 服务器拓扑结构如图 5-3-3 所示。

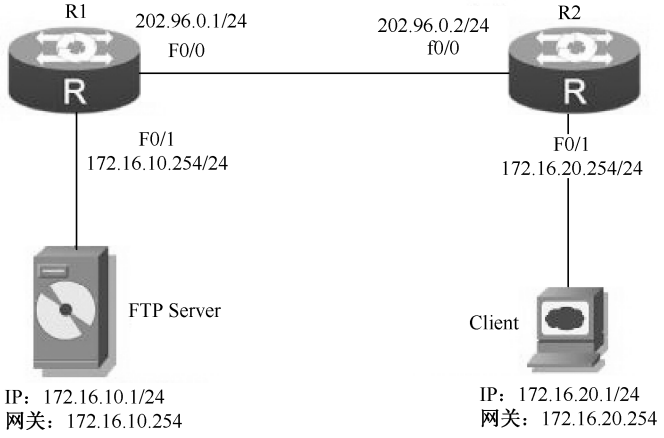


图 5-3-3　发布 FTP 服务器拓扑结构

IP 地址配置表见表 5-3-2。

表 5-3-2　IP 地址配置表

设　　备	IP 地址	网　　关
R1 的 F0/0	202.96.0.1/24	
R1 的 F0/1	172.16.10.254/24	
R2 的 F0/0	202.96.0.2/24	
R2 的 F0/1	172.16.20.254/24	
FTP Server	172.16.10.1 /24	172.16.10.254
Client	172.16.20.1/24	172.16.20.254

学习小结

本学习活动使用静态 NAT 技术实现了向外网发布内网服务器的功能。常见的网络应用程序通常使用默认端口，利用 NAPT 可以给这些端口和内网服务器的私有地址建立映射，从而在保证内网主机访问因特网的基础上，实现使用单个公网地址发布多个网络服务器的目的。

学习活动 2　利用动态 NAT 实现局域网访问互联网

内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

学习情境

某公司向电信运营商申请了专线接入和公网 IP 地址，这意味着公司可以访问 Internet 了。然而，公司只有一个公网 IP 地址，却有几十台等待联网的计算机。

情境分析

公司内部有很多台主机都要接入外网，而公司只向 ISP 申请了一个合法的 IP 地址。可以使用基于动态 NAT 地址复用（NAPT）使多个用户同时共用一个合法的 IP 地址与外部 Internet 进行通信。

当路由器检测到公司内部计算机访问外网的数据包时，会将 IP 数据包头部中的源 IP 地址（即内部保留地址）转换为公司申请的公网 IP（内部全局地址）地址。经过 IP 地址转换的数据包就可以路由到 Internet 上了。

所需设备。

（1）DCR-2600 路由器 2 台。

（2）CR-V35MT 1 条。

（3）CR-V35FC 1 条。
（4）Console 线 1 条。
（5）交叉线 2 条。
（6）PC 2 台。
使用 NAPT 访问 Internet 的拓扑结构如图 5-3-4 所示。

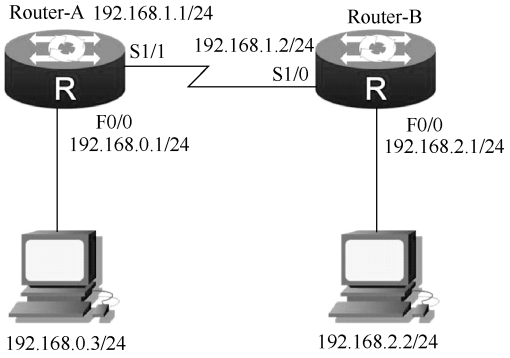


图 5-3-4　使用 NAPT 访问 Internet 的拓扑结构

IP 地址配置表见表 5-3-3。

表 5-3-3　IP 地址配置表

设　　备	IP 地址	网　　关
Router-A 的 S1/1	192.168.1.1/24	
Router-A 的 F0/0	192.168.0.1/24	
Router-B 的 S1/0	192.168.1.2/24	
Router-B 的 F0/0	192.168.2.1/24	
Web Server	192.168.2.2/24	192.168.2.1
Client	192.168.0.3/24	192.168.0.1

相关知识

NAPT 又称为 PAT 或者端口级复用 NAT，是动态 NAT 的一种实现形式，常用于公网地址端极缺乏、甚至只有一个公网地址的末节网络中。

在 NAPT 转换中，路由器或者防火墙通常将数据包的源 IP 地址和源端口进行转换。NAPT 设备使用不同的端口号来识别内部主机。

NAPT 设备使用 IP ACL 识别需要进行地址转换的数据流，将数据包的源 IP 地址（内部私有地址）和端口地址转换为公网地址，并路由到因特网中。这次转换会在 NAPT 设备的 NAT 地址转换表中产生一条记录。当 NAPT 设备收到外部网络发送的应答数据包后，根据 NAT 转换表的记录，设备识别出数据包中的端口号对应的内部主机，将应答数据包中目的 IP 地址（即内部公网地址）转换为原来的内部私有地址，并将该数据包转发到内部网络中。由于它有两个方向上的地址转换，NAPT 向外屏蔽了内部主机的地址信息，在一定程度上加强了内部网络的安全性。

NAT 是指将网络地址从一个地址空间转换为另一个地址空间的行为。NAT 将网络划分为内部网络（Inside）和外部网络（Outside）两部分。局域网主机利用 NAT 访问网络时，是将局域网内部的本地地址转换为全局地址（互联网合法 IP 地址）后转发数据包。

一般而言，有两种技术可以实现使用有限的甚至只有一个公网 IP 地址来满足大量的主机访问因特网的需求，它们是代理服务器技术和网络地址转换技术（NAT）。其中，NAT 在大量的末节网络中的应用最为普遍。

NAT 技术常使用各类术语如下。

（1）内部本地地址：通常指分配给内部主机使用的私有地址。

（2）内部全局地址：由 ISP 提供的用于本网络使用的公网地址。

（3）外部本地地址：通常指提供给外部网络使用的私有地址。

（4）外部全局地址：外部网络使用的可路由的公网地址。

（5）外部端口：内部网络中运行 NAT 机制的设备，如路由器、防火墙等，用于连接外网的接口。

（6）内部端口：运行 NAT 机制的设备用于连接内网的接口。

NAT 通常包括以下几种应用类型。

（1）静态 NAT：由管理员手工进行设置，其方式为一对一的私有地址和公网地址之间的转换。

（2）动态 NAT：由设备自动进行，其方式为一段内部地址和一个外部地址池之间进行转换，每次转换都是一对一进行的。

（3）静态 NAPT：由管理员手工设定，用于将一个内部私有地址和端口号转换为一个公网地址和端口号。静态 NAPT 可以实现一个公网地址的复用。

（4）动态 NAPT：由设备自动进行，利用不同的端口号来将多个私有地址转换为一个公网地址。

（5）NAT 实现 TCP 均衡：使用 NAT 机制创建一台虚拟主机并提供 TCP 服务，该虚拟主机对应内部多台实际的主机，然后对目的地址进行轮询置换，达到负载分流的目的。

动态 NAPT 是最为常见的 NAT 应用。一般情况下，配置 NAPT 应遵循以下步骤。

（1）定义外网端口。

（2）定义内网端口。

（3）定义需要进行地址转换的数据流（使用 IP ACL 来定义）

（4）定义公网地址池。

（5）建立数据流和公网地址池之间的映射关系。

（6）添加指向外网的静态路由。

步骤实现

步骤 1：按照图 5-3-4 连接网络拓扑结构。

步骤 2：按照表 5-3-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：恢复路由器的出厂配置。

```
Router>enable                                          ！进入特权模式
Router#2004-1-1 00:32:10 User DEFAULT enter privilege mode from console 0,
```

```
level = 15
    Router#delete                                          ！删除配置文件
    this file will be erased,are you sure?(y/n)y
    Router#reboot                                          ！重新启动
    Do you want to reboot the router(y/n)?y
    Please wait…
```

步骤 4：在 Router-A 上设置接口 IP 地址、DCE 的时钟频率。

```
    Router>enable                                          ！进入特权模式
    Router #config                                         ！进入全局配置模式
    Router _config#hostname Router-A                       ！修改机器名称
    Router-A_config#interface s1/1                         ！进入接口模式
    Router-A_config_s1/0#ip address 192.168.1.1 255.255.255.0！配置IP地址
    Router-A_config_s1/0#physical-layer speed 64000   ！配置DCE时钟频率
    Router-A config s1/0#no shutdown
    Router-A_config_s1/0# ^Z
```

步骤 5：在 Router-B 上设置 IP 地址。

```
    Router>enable
    Router#config
    Router config#hostname Router-B
    Router-B_config#interface s1/0
    Router-B_config_s1/0#ip address 192.168.1.2 255.255.255.0
    Router-B config s1/0#no shutdown
    Router-B_config_s1/0#^Z
```

步骤 6：配置 Router-A 的 NAT。

```
    Router-A#conf
    Router-A_config#ip access-list standard 1 ！定义访问控制列表
    Router-A config std nacl#permit 192.168.0.0 255.255.255.0
                                          ！定义允许转换的源地址范围
    Router-A config std nacl#exit
    Router-A config#ip nat pool overld 192.168.1.10 192.168.1.20 255.255.255.0
            ！定义名为overld的转换地址池
    Router-A config#ip nat inside source list 1 pool overld overload
                ！配置将ACL允许的源地址转换成overld中的地址，并且做PAT的地址复用
    Router-A_config#int f0/0
    Router-A_config_f0/0#ip nat inside         ！定义f0/0为内部接口
    Router-A config f0/0#int s1/1
    Router-A_config_s1/1#ip nat outside            ！定义s1/1为外部接口
    Router-A config s1/1#exit
    Router-A_config#ip route 0.0.0.0 0.0.0.0 192.168.1.2 ！配置路由器A的默认路由
```

步骤 7：查看 Router-B 的路由表。

```
    Router-B#sh ip route
    Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
    D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
    ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
```

```
    OE1 - OSPF external type 1, OE2 - OSPF external type 2
    DHCP - DHCP type
    VRF ID: 0
    C 192.168.1.0/24 is directly connected, Serial1/0
    C 192.168.2.0/24 is directly connected, FastEthernet0/0
                                    ！注意：并没有到192.168.0.0的路由
```

步骤 8：测试网络连通情况，如图 5-3-5 所示。

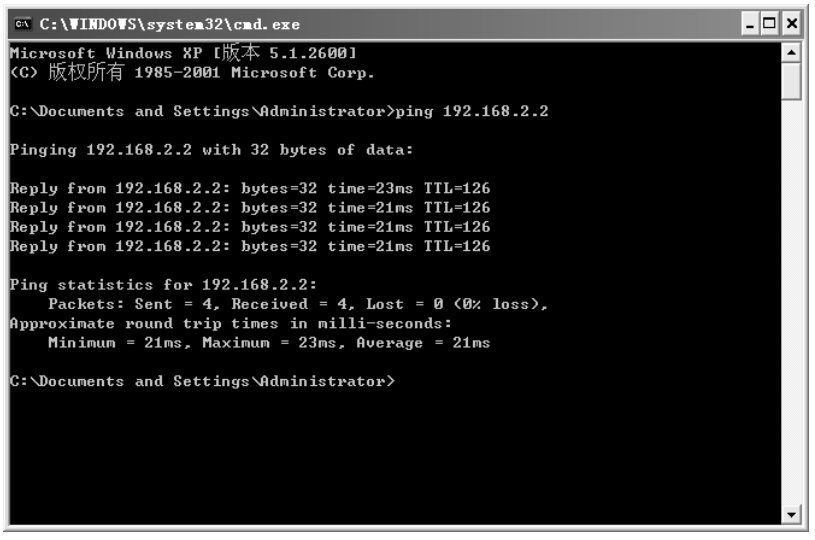

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=23ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 21ms, Maximum = 23ms, Average = 21ms
C:\Documents and Settings\Administrator>

图 5-3-5　测试效果图

步骤 9：查看 Router-A 的地址转换表。

```
    Router-A#sh ip nat translation
    Pro. Dir  Inside local       Inside global     Outside local       Outside
global
    ICMP OUT 192.168.0.3:512  192.168.1.10:12512  192.168.1.2:12512    192.168.
1.2:12512
```

小贴士

（1）注意转换的方向和接口，不要把 Inside 和 Outside 应用的接口弄错。

（2）注意地址池、ACL 的名称。

（3）在 Router-B 中一定不能加指向 192.168.0.0 网络的回指路由，否则将无法判断连通性是否为由 NAT 的设置成功引起的。

课堂训练

在 R2 的 F0/0 接口上添加 ACL，禁止来自网段 192.168.0.0/24 的数据包。在 R1 路由器上配置 NAPT，使得左侧内部主机 PC1 可以通过公网访问右侧的 Web Server。

所需设备：

（1）DCR-2600 路由器 2 台。

（2）PC 2 台。

（3）Console 线 1 条。

（4）双绞线 3 条。

NAPT 训练用图如图 5-3-6 所示。

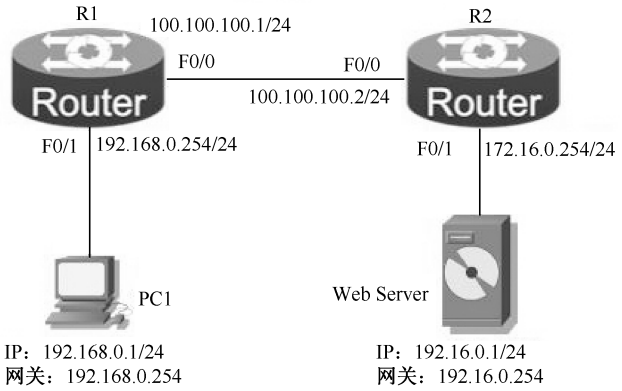


图 5-3-6　NAPT 训练用图

IP 地址配置表见表 5-3-4。

表 5-3-4　IP 地址配置表

设　　备	IP 地址	网　　关
R1 的 F0/0	100.100.100.1/24	
R1 的 F0/1	192.168.0.254/24	
R2 的 F0/0	100.100.100.2/24	
R2 的 F0/1	172.16.0.254/24	
PC1	192.168.0.1 /24	192.168.0.254
Web Server	172.16.0.1/24	172.16.0.254

学习小结

本学习活动在末节网络的路由器上使用 NAPT 技术，实现了内部网络主机通过公网地址复用来访问因特网的功能。NAPT 是网络地址转换众多应用中最为常见的一种。相对于其他的应用模式而言，NAPT 使用更少的公网地址、支持更多的内部主机。NAPT 还向外屏蔽了内部网络的结构，提高了网络安全性。

项目考核

1．配置 PPP 协议，连接办事处和公司总部，如图 5-3-7 所示。

（1）使用 PPP 协议。

（2）使用 CHAP 方式认证用户。

完成标准：PPP 连接能够正常建立，办事处和公司总部间路由器可以相互连通。

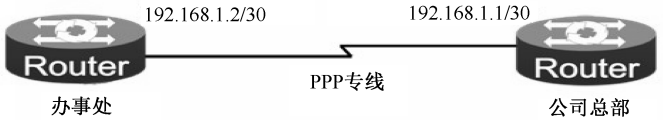


图 5-3-7　PPP 专线

2．配置 NAPT，公司只有一个公网 IP 地址，却有几十台等待联网的计算机，解决某公司接入互联网公网 IP 地址不足的情况，如图 5-3-8 所示。

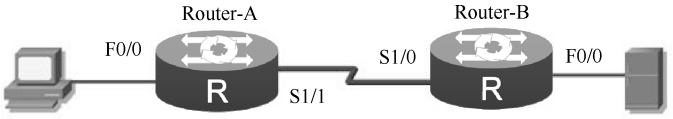
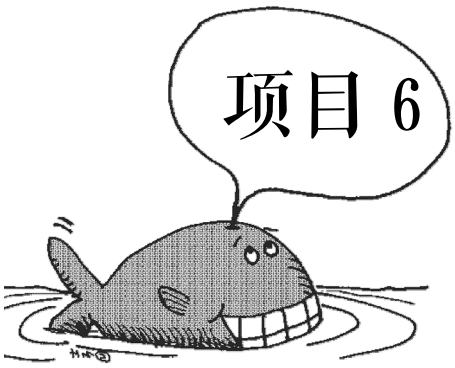


图 5-3-8　公司网络拓扑图

设备配置信息表见表 5-3-5。

表 5-3-5　设备配置信息表

Router-A		Router-B	
F0/0	192.168.0.1/24	F0/0	192.168.2.1/24
S1/1　(DCE)	192.168.1.1/24	S1/0	192.168.1.2/24
PC		Server	
IP 地址	192.168.0.3/24	IP	192.168.2.2/24
网关	192.168.0.1	网关	192.168.2.1



无线网络配置

项目学习说明

“无线”代表一种生活方式，它改变着我们的工作和生活。作为有线网络的延伸，无线网络未来会成为云时代的主要信息载体。大多初学者体验过无线上网的轻松与惬意，但无线网络配置与管理又显得非常神秘。无线局域网的搭建、接入与安全管理，都是网络学习者必备的知识和技能。

本项目重点学习瘦 AP 模式的无线网络的基本配置、无线 AC 的 DHCP 服务管理和无线 AC 的安全控制。

学习能力目标

学习任务 1 瘦 AP 模式的无线网络的基本配置
学习任务 2 无线 AC 的 DHCP 服务管理
学习任务 3 无线 AC 的安全控制

职业能力目标

- 熟练掌握瘦 AP 模式无线网络的配置方法和步骤
- 熟练掌握 AC 的工作原理
- 理解无线 AC 的 DHCP 管理的概念
- 理解无线 AC 的安全控制
- 熟悉 AC 安全控制的实现方法

学习任务 1　配置瘦 AP 模式的无线网络

无线 AP（Access Point）即无线接入点，也称无线网桥、无线网关。瘦 AP 是指需要无线

接入控制器（AC）进行管理、调试和控制的 AP，不能独立工作，必须与 AC 配合使用。

学习情境

公司购置了一批无线网络设备和终端，准备搭建自己的无线局域网，在原有网络投资有效的基础上，扩充网络规模。

情境分析

该项目规划与实施前，要认真分析无线设备的技术、了解网络组件的功能，搭建出符合客户需求的无线网络，做出正确高效的设备配置，并启用相应的安全手段，保障无线网络的正常运行。

将 AC 和无线 AP 直连，实现管理和数据转发，即可传输用户 VLAN 的数据。方法：采用 AC+FIT AP 方案，使用二层注册的方式，在 AC 上进行配置，广播一个 SSID，提供开放式接入。

无线 AP 和无线 AC 通过 VLAN1（192.168.1.0/24）进行关联，无线用户通信为 VLAN10（192.168.10.0/24），无线用户和 AP 的网关都在 AC 上。广播 SSID 为 DCN，关联到 VLAN10。

所需设备：

（1）DCWS-6028 无线接入控制器 1 台。

（2）DCWL-7962AP（R3）1 台。

（3）带有无线网卡的笔记本式计算机 2 台。

（4）直连线 1 条。

（5）AC 的 Console 线 1 条。

学习活动拓扑结构如图 6-1-1 所示。

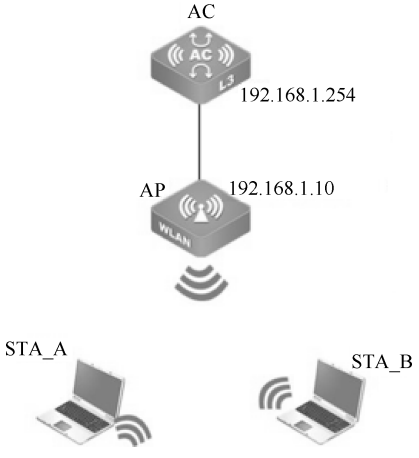


图 6-1-1　开放式无线网络接入

相关知识

无线局域网（Wireless Local Area Network，WLAN）通常缩写为 WLAN，指应用无线通

信技术将计算机设备互连起来，构成可以互相通信和实现资源共享的网络体系。WLAN 无线传输遵循 IEEE 802.11 体系的标准，支持 IEEE 802.11a/b/g/n，理论传输速率最高可以达到 600Mb/s。

WLAN 相对于有线网络的优势在于组网灵活、移动方便、节省布线成本 ，WLAN 相对于有线网络的缺点是容易受到干扰、速度较低、数据容易被窃取。

1．IEEE 802.11 协议

无线技术使用电磁波在设备之间传送信息。电磁波是通过空间传送无线电信号的一种介质。802.11 WLAN 是一套 IEEE 标准，该标准定义了如何使用免授权的工业、科学和医疗 (ISM) 射频 (RF) 频段作为无线链路传输和控制网络信号。802.11 标准利用 2.4GHz 和 5GHz 频带的电磁波进行信号传输， 802.11 无线标准家族包括 802.11a/b/g/n/ac 五个标准，我们经常见到的是 802.11a/b/g/n 四个标准， 比较陌生的是 IEEE 802.11ac，它是继 802.11n 之后的新通过的版本，于 2013 年 12 月获批，工作在 5GHz 频段，理论上可以提供高达 1Gb/s 的数据传输能力，见表 6-1-1。

表 6-1-1　802.11 协议标准介绍

	802.11a	802.11b	802.11g	802.11n	802.11ac
工作频段	5GHz	2.4GHz	2.4GHz	2.4GHz 和 5GHz	5GHz
信道数	最多 23	3	3	最多 14	最多 23
调制技术	OFDM	DSSS	DSSS 和 OFDM	MIMO-OFDM	MIMO-OFDM
数据传输速率	＜54Mb/s	＜11Mb/s	＜54Mb/s	最高可达 600Mb/s	可达 3.7Gb/s
发布时间	1999 年	1999 年	2003 年	2009 年	2013 年 12 月

2．Wi-Fi 概念

Wi-Fi 是 Wi-Fi 联盟制造商的商标，可作为产品的品牌认证，是一个建立于 IEEE 802.11 标准的无线局域网络设备，是目前应用最为普遍的一种短程无线传输技术。基于两套系统的密切相关，也常有人把 Wi-Fi 当做 IEEE 802.11 标准的同义词，其标识如图 6-1-2 所示。

图 6-1-2　Wi-Fi 标识

Wi-Fi 在无线局域网的范畴是指“ 无线相容性认证 ”，实质上是一种商业认证，也是一种无线联网的技术，以前通过网线连接计算机，而现在则通过无线电波来联网。常见的是无线路由器，在这个无线路由器的电波覆盖的有效范围内都可以采用 Wi-Fi 连接方式进行联网，

如果无线路由器连接了一条 ADSL 线路或者其他线路，则其又被称为“热点”。

3. WLAN 频段和信道

WLAN 只使用 2.4GHz 频段和 5GHz 频段，这两个频段的特性和使用情况不同。

2.4GHz 无线技术是一种短距离无线传输技术，供免费使用。2.4GHz 是全世界公开通用的无线频段，蓝牙技术即工作在这一频段。在 2.4GHz 频段下工作可以获得更大的使用范围和更强的抗干扰能力。

目前对于 2.4GHz 信道的使用情况如下。

北美地区：1～11。

中国、欧洲：1～13。

日本：1～13，14（仅适用于 802.11b）。

其中在中国有 13 个信道可用，每个信道有 20MHz 带宽，每隔 5MHz 有一个频点。

5GHz 频段是一个比 2.4GHZ 频率更高、开放的 ISM 频段，最近几年开始进入产品研发领域，它遵从于 802.11a 等国际标准，目前少数鼠标及无线电话使用此技术，是有望代替 2.4GHz 无线技术的技术之一，中国 WLAN 工作的频率是 5.725～5.850GHz。在此频率范围内又划分了五个信道，信道间隔 20MHz，信道宽度 20MHz，从中心频率左右扩展 10MHz。

4. WLAN 组网模式

（1）Ad-hoc 模式：如图 6-1-3 所示，这就是所谓的点对点直接通信模型。这种组网模式不需要使用无线接入点，无线信号直接从一台计算机到另一台计算机。

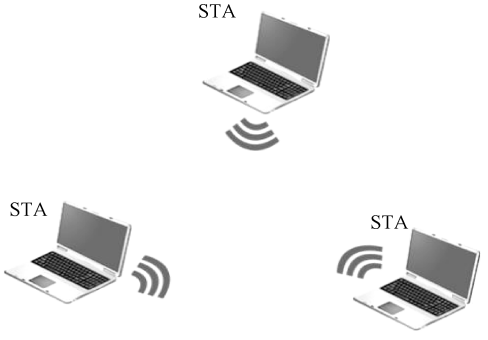


图 6-1-3　Ad-hoc 组网模式

（2）Infrastructure 模式：如图 6-1-4 所示，也称集中管理模式，需要 AP 提供接入服务，所有 STA 关联到 AP 上，访问外部以及 STA 之间交互的数据均由 AP 负责转发。

图 6-1-4　Infrastructure 模式

（3）中继模式：如图 6-1-5 所示，也称桥接模式，即两个或多个网络（LAN 或 WLAN）

或网段，通过无线中继器、无线网桥或无线路由器等无线网络互连设备连接起来。

图 6-1-5　中继模式

AP 工作在瘦模式时需要注册到 AC 上，成功注册后才能接受 AC 的统一管理，这个过程也称 AP 上线。

有两种注册方式：AC 发现 AP，AP 处于被动发现状态；AP 发现 AC，即在 AP 上指定 AC 的 IP 地址。

AC 主动发现 AP 时有三种情况：在 AC 上添加 AP 的数据库，即 AP 的 MAC 地址；如果使用三层发现，则把 AP 的 IP 地址添加到 IP-list 中；如果使用二层发现，则把 AP 所在的 VLAN ID 添加到 VLAN-list 中。

AP 主动发现 AC，需要在 AP 上添加静态的 AC 的无线地址，或者 AP 通过 DHCP 方式获取 AC 列表（利用 option 43 选项）。

步骤实现

步骤 1：配置无线 AC 的端口相关信息。

```
DCWS(config)#interface e1/0/1
DCWS(config-if-ethernet1/0/1)#speed-duplex force10-full
！更改接口的速度和双工为10Mb/s全双工
DCWS(config-if-ethernet1/0/1)#switchport mode trunk
！该链路需要承载多个VLAN数据时，需要将此链路模式更改为Trunk模式
DCWS(config-if-ethernet1/0/1)#switchport trunk native vlan 1
！使VLAN1通过Trunk链路时不打vlan tag，如果AP处于除VLAN1，则其他VLAN需要把本征
！VLAN更改成该VLAN
```

步骤2：配置VLAN，创建用户VLAN，AP和AC互连VLAN。

```
DCWS(config)#vlan 1                              ！AP和AC所在VLAN
DCWS(config-vlan)#name Dcn_ap_ac                 ！VLAN!名称是Dcn_ap_ac
DCWS(config-vlan)#vlan 10                        ！无线用户所在vlan
DCWS(config-vlan)#name Dcn_sta                   ！VLAN 10名称是Dcn_sta
```

步骤3：配置AP和STA的网关地址。

```
DCWS(config)#interface vlan 1                          ！配置AP的网关
```

```
DCWS(config-if-vlan1)#ip address 192.168.1.254 255.255.255.0
DCWS(config)#interface vlan 10                          !配置STA的网关
DCWS(config-if-vlan1)#ip address 192.168.10.254 255.255.255.0
```

步骤4：配置AP的DHCP服务器。

```
DCWS(config)#service dhcp                               !开启DHCP服务
DCWS(config)#ip dhcp pool Dcn_ap                        !创建DHCP地址池Dcn_ap
DCWS(dhcp-wireless ap-config)#network 192.168.1.0 255.255.255.0
!分配给AP的地址网段
DCWS(dhcp-wireless_ap-config)#default-router 192.168.1.254   !分配给AP的网关
```

步骤5：配置STA的DHCP服务器。

```
DCWS(config)#ip dhcp pool Dcn_sta                       !创建DHCP地址池Dcn_sta
DCWS(dhcp-wireless_sta-config)#network 192.168.10.0 255.255.255.0
!分配给无线用户的地址网段
DCWS(dhcp-wireless sta-config)#dns-server 114.114.114.114 114.114.115.115-
!分配给无线用户的DNS地址
DCWS(dhcp-wireless sta-config)#default-router 192.168.10.254
!分配给无线用户的网关地址
```

步骤6：查看AP获取的地址的相关信息。

```
DCWS#show ip dhcp binding
Total dhcp binding items: 1, the matched: 1
IP address        Hardware address        Lease expiration        Type
00-03-0F-19-99-80          Sun Jun 15 12:55:00 2014         Dynamic
```

步骤7：开启无线功能。

```
DCWS(config)#wireless                                   !进入无线配置模式
DCWS(config-wireless)#enable                            !开启无线功能，默认是关闭的
```

小贴士

关闭无线功能的命令是 no enable。

查看当前无线功能是否开启的命令是“show wireless”，“Administrative Mode”显示的是无线功能是否开启。

```
DCWS(config-wireless)#no enable
DCWS#show wireless
Administrative Mode.......................... Enable
```

步骤8：指定VLAN发现列表。

```
DCWS(config-wireless)#discovery vlan-list 1
!AC发现AP的所在的VLAN，默认为VLAN 1
```

小贴士

查看 AC 发现模式的命令是“show wireless discovery”。

```
DCWS#show wireless discovery
```

查看 AC 二层发现 VLAN 列表的命令是“show wireless discovery vlan-list”。

```
DCWS#show wireless discovery vlan-list
```

步骤9：配置无线IP地址。

```
DCWS(config-wireless)#static-ip 192.168.1.254      ！指定静态无线地址
DCWS(config-wireless)#no auto-ip-assign             ！关闭无线地址自动选举功能
```

小贴士

无线 IP 地址的配置方式有动态选取和静态指定两种，动态选取的 IP 地址优先级高于静态指定的 IP 地址的优先级。建议项目实施时采用静态指定无线 IP 地址的方式，防止动态选取时 IP 地址变化导致无线网络中断。动态选取无线 IP 地址的原则：优先选择接口 ID 小的 loopback 接口的地址，未配置 loopback 接口时优先选择接口 ID 小的三层接口 IP 地址（注意，不是 IP 地址小的接口）。

步骤 10：验证 AC 选取的无线 IP 地址是否正确。

```
DCWS#show wireless
Administrative Mode.......................... Enable         ！正确状态
Operational Status........................... Enabled        ！正确状态
WS IP Address................................ 192.168.1.254  ！无线IP地址
WS IPv6 Address.............................. -----
WS Auto IP Assign Mode ................... Disable
！无线IP地址自动分配模式的状态为禁止
WS Switch Static IP ......................... 192.168.1.254
！无线交换机静态IP地址
WS Switch Static IPv6 ....................... -----
！无线交换机静态IPv6地址为空
AP Authentication Mode....................... None
！AP认证模式为不认证
```

步骤 11：验证 AP 注册状态。

```
DCWS#show wireless ap status
DCWS(config-wireless)#ap datebase 00-03-0F-19-99-80
！手工添加该MAC地址到AC的MAC地址认证数据库
DCWS(config-wireless)#ap authentication none
!AP认证方式为不认证，取消MAC地址认证
```

步骤 12：配置 SSID。

```
DCWS(config-wireless)#network 1                     ！创建Network 1
DCWS(config-network)#ssid DCN                       ！无线信号（Wi-Fi名称）DCN
DCWS(config-network)#vlan 10
！指定network 1在VLAN 10下，如果用户VLAN与管理VLAN相同，则此处不需要配置，默认是管理
！VLAN，建议管理VLAN和用户不要重复
```

步骤 13：下发 profile 配置。

```
DCWS#wireless ap profile apply 1
Configured profile is not valid to apply for AP:00-03-0f-18-c7-00, due to
```

```
hardware type mismatch!!
    ！系统提示配置下发失败，原因是硬件类型不匹配，需要修改profile对应的硬件类型。
```

步骤 14：需要修改 profile 对应的硬件类型。

```
DCWS(config-wireless)#ap profile 1
DCWS(config-ap-profile)#hwtype 1            ！更改硬件类型为1
DCWS#show wireless ap status
   MAC Address                                  Configuration
 (*) Peer Managed    IP Address    Profile Status     Status          Age
---------------- -------------- ------- ------- ------------- -----------
00-03-0F-19-99-80 192.168.1.10    1      ManagedSuccess   0d:00:00:04
Total Access Points.......................... 1
！配置下发成功后Status显示为Success
```

小贴士

（1）下发配置前需注意当前无线网络的使用情况，防止无线网络中断。

（2）同一 profile 只能对应一个硬件类型，即如果网络中存在多个型号的 AP，则需创建多个 profile。

步骤 15：开启 VAP。radio 下需要启用对应的 VAP，network2 对应 vap 1，所以要把 vap 1 开启。

```
DCWS(config-ap-profile)#radio 1
DCWS(config-ap-profile-radio)#vap 0
DCWS(config-ap-profile-radio)#enable
！默认情况只有vap0 开启，其他VAP需要手动开启
DCWS(config-ap-profile-vap)#network 1            ！为VAP0关联一个network 1
DCWS(config-ap-profile-vap)#enable
！默认情况只有network1 开启，其他network需要手动开启
DCWS#wireless ap profile apply 1
！每次更改AC配置后一定要重新下发，否则配置更新不会作用在AP上
```

步骤 16：验证测试，用笔记本式计算机连接搜索到的 SSID 为 dcn_wlan 的无线信息，输入验证密码，连接成功并获取到 IP 地址。

学习小结

本任务主要学习如何实现瘦 AP 模式的无线网络的配置，实现了数据的传输接收，并把无线 SSID 信号广播出去，让客户端能在覆盖区域接收到并通过验证密码连接进去，实现无线网络办公学习。

学习任务 2　无线 AC 的 DHCP 服务管理

在很多大型网络环境中会使用到三层交换机，而 AC 自带的 DCHP 服务器仅能够在同一个局域网内给 AP 分配 IP 地址，在有三层交换机的环境下可以通过配置外接 DHCP 服务器给 AP 分配 IP 地址。

学习情境

由于公司业务规模的扩大，公司进行了网络中心的扩容。在无线局域网部署时，需要配置 AC 为 AP、无线用户所在的数据 VLAN 提供 IP 地址分配功能，以保障 AP 与 AC 的通信及无线用户的数据转发。

情境分析

将无线 AC 和三层交换机相连，下面接无线 AP，实现管理和数据转发，即可传输用户 VLAN 的数据。采用 AC+FIT AP 方案，采用三层注册的方式，在 AC 上进行配置，广播一个 SSID，提供开放式接入。

无线 AP 和无线 AC 通过 VLAN1 192.168.1.0/24 进行关联，无线用户通信为 VLAN30（192.168.3.0/24），无线用户和 AP 的网关都在 AC 上，AP 所在 VLAN 为 VLAN10（192.168.1.0/24）。广播 SSID 为 DCN，关联到 VLAN30 上。

所需设备：

（1）DCWS-6028 无线 AC1 台。

（2）DCWL-7962AP(R3)1 台。

（3）DCRS-5650 交换机 1 台。

（4）带有无线网卡的笔记本式计算机 2 台。

（5）Console 线 1 条。

（6）直连线 2 条。

无线 AC 的 DHCP 服务管理拓扑结构如图 6-2-1 所示。

图 6-2-1　无线 AC 的 DHCP 服务管理拓扑结构

相关知识

DHCP 功能的典型应用有两个：一是配置 DHCP option 43 功能，在 AP 三层注册时能够让 AP 跨越三层设备找到 IP 地址不在同一网段的 AC，此时要求网络的三层是相通的；二是配置 WLAN 时为无线 AP 及 STA 分配 IP 地址，这种应用需要先开启 AC 的 DHCP 服务，再分别为各个 VLAN 定义地址池和网关地址，推送 DNS 服务地址。

步骤实现

步骤 1：无线 AC 的配置。

```
DCWS(config)#service dhcp                    ！开启DHCP服务器
DCWS(config)#ip dhcp pool Wireless_ap        ！创建DHCP地址池，名称为Wireless_ap
DCWS(dhcp-wireless ap-config)#network 192.168.1.0 255.255.255.0
！分配给AP的地址网段
DCWS(dhcp-wireless ap-config)#option 43 ip 1.1.1.1
！下发给AP的dhcp option43用于AP寻找AC，所以要保证网络的三层可达
DCWS(dhcp-wireless_ap-config)#default-router 192.168.1.254
！分配AP的默认网关地址
DCWS(config)#ip dhcp pool Wireless sta
！创建DHCP地址池，名称为Wireless_sta
DCWS(dhcp-wireless sta-config)#network 192.168.3.0 255.255.255.0
！分配给无线用户的地址网段
DCWS(dhcp-wireless_sta-config)#dns-server 114.114.114.114  114.114.115.115
！分配给无线用户的DNS地址
DCWS(dhcp-wireless sta-config)#default-router 192.168.3.254
！分配给无线用户的默认网关地址
```

步骤 2：三层交换机的配置。

```
DCRS-5650-28>
DCRS-5650-28>enable
DCRS-5650-28#config
DCRS-5650-28(config)#hostname  WS
WS(config)#vlan 10                           ！定义VLAN10
WS(config)#vlan 30                           ！定义VLAN30
WS(config)#int vlan 10                       ！打开VLAN10数据通道
WS(config-vlan10)#no shutdown
WS(config)#int vlan 30                       ！打开VLAN30数据通道
WS(config-vlan30)#no shutdown
```

小贴士

（1）无线部分的配置与前一学习任务相同。

（2）无线部分配置完成后不要忘记下发配置给 AP。

知识拓展

1. AP 用户数调整

当无线网络中无线终端数量众多，AP 性能较差，或者网速较慢时，需要对 AP 用户数量进行限制，避免 AP 中用户数过多影响性能及用户体验。单个 AP 限制多少用户需要根据客户需求确定。

（1）进入 network 配置模式。

```
DCWS(config)#wireless
DCWS(config-wireless)#network 1
DCWS(config-network)# max-clients 10 ！更改最大客户端数，默认为25个（取值0～200）
```

（2）进入 Radio 配置模式.

```
DCWS(config-wireless)#ap profile 1
DCWS(config-ap-profile)# radio 1
DCWS(config-ap-profile-radio)# max-clients 10
                                        !更改最大客户端数，默认为25个（取值0～200）
```

2. AP 射频管理

射频管理主要是对射频参数的设置，具体配置步骤如下。

（1）设置国家代码。

```
DCWS(config-wireless)#country-code cn ！设置国家代码为China
```

（2）调整射频工作模式。

```
DCWS(config-wireless)#ap profile 1
DCWS(config-ap-profile)#radio 1
DCWS(config-ap-profile-radio)#mode ?
DCWS(config-ap-profile-radio)#mode bg-n！设置为支持802.11b、802.11g、802.11n
```

（3）设置 AP 功率和信道。

```
DCWS(config-wireless)#ap database 00-03-0F-19-99-80      ！管理单个AP
DCWS(config-ap)#radio 1 channel 11          ！调整radios1工作在11信道
The valid AP entry is updated. This AP is already managed, to update the managed
AP configuration with the new value(s) you need to reset the AP.
DCWS(config-ap)#radio 1 power 50            ！调整radio射频功率为50%，默认为100%
```

学习小结

本任务主要学习无线 AC 的 DHCP 服务管理，实现了三层交换机的环境下 AC 和 AP 的无线连接，实现了无线网络办公环境。

学习任务 3　无线 AC 的安全控制

无线网络中的威胁包括 AP 威胁、Client 威胁，可以采取的安全策略包括动态黑名单、黑

名单/白名单、ARP 抑制等。

学习情境

公司无线网络部署完成，基本功能都能满足客户需求。AC 作为无线网络的配置核心，需要检测网络中的威胁、建立安全策略保护无线 AC 的安全，以满足公司的安全需要。

情境分析

配置动态黑名单，即检测到某个终端设备发送泛洪报文超过安全阈值时，将该终端设备添加到黑名单列表中。AP 使用该列表，丢弃该名单中的终端设备发送的数据帧。

根据熟悉的无线终端的 MAC 地址，分别设置白名单和黑名单，分别控制无线终端的允许和禁止接入。

所需设备：

（1）DCWS-6028 无线 AC1 台。

（2）DCWL-7962AP（R3）1 台。

（3）带有无线网卡的笔记本式计算机 2 台。

（4）Console 线 1 条。

（5）直连双绞线 1 条。

AC 的安全控制拓扑结构如图 6-3-1 所示。

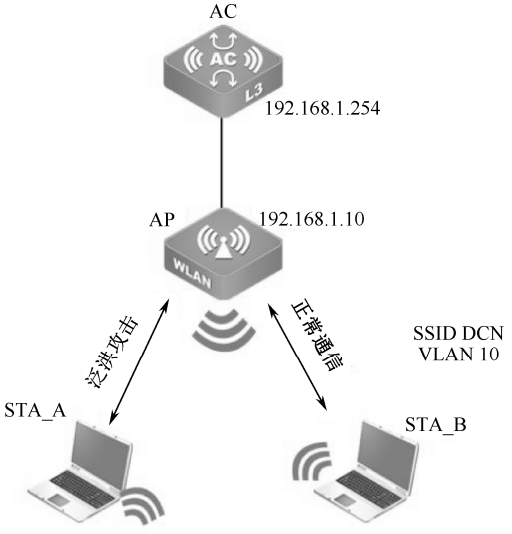


图 6-3-1　AC 的安全控制拓扑结构

相关知识

动态黑名单（Dynamic Blacklist）属于无线安全功能模块中防 DOS 攻击的部分。动态黑名单中包含将被丢弃帧的终端设备的 MAC 地址。AP 使用该列表，丢弃该名单中的终端设备发送的数据帧。当检测到某个终端设备发送的泛洪报文超过安全阈值时，将该终端设备添加

到黑名单中。

相关命令详解：

```
DCWS(config-wireless)#mac-authentication-mode ?
  black-list                ！设置MAC认证模式为黑名单列表
  white-list                ！设置MAC认证模式为白名单列表
DCWS(config-wireless)#mac-authentication-mode white-list
DCWS(config-wireless)#known-client ?
  FF-FF-FF-FF-FF-FF         ！输入已知的客户端MAC地址
DCWS(config-wireless)#known-client ff-ff-ff-ff-ff-ff ?
  Action                    ！配置一个已知的客户端认证行为
  Name                      ！配置一个已知的客户端名
DCWS(config-wireless)#known-client ff-ff-ff-ff-ff-ff action ?
  deny                      ！设置已知客户端认证动作为拒绝
  global-action             ！设置已知客户端认证动作为全局动作
  grant                     ！设置已知客户端认证动作为批准
DCWS(config-wireless)#known-client EC-A8-6B-39-80-D1 action global-action
DCWS(config-wireless)#network 1
DCWS(config-network)#mac authentication ?
  local                     ！利用AP profile列表设置客户端MAC认证
  radius                    ！利用RADIUS服务器进行客户端MAC认证
DCWS(config-network)#mac authentication local
```

步骤实现

步骤 1：配置动态黑名单

```
DCWS-6028 (config)# wireless
DCWS-6028 (config-wireless)# no wids-security client threshold-interval-auth
DCWS-6028 (config-wireless)# wids-security client threshold-value-auth 6000
DCWS-6028 (config-wireless)# wids-security client configured-auth-rate
DCWS-6028 (config-wireless)#dynamic-blacklist          ！开启动态黑名单功能
DCWS-6028 (config-wireless)#dynamic-blacklist lifetime 600
DCWS-6028 (config-wireless)#network 100
DCWS-6028 (config-network)#mac authentication local   ！本地MAC认证功能
```

步骤 2：配置黑名单/白名单。

（1）允许无线终端接入列表。

```
DCWS-6028 (config-wireless)#mac-authentication-mode white-list   !白名单列表
DCWS-6028 (config-wireless)#known-client 00-6-11-6-11-11 action
global-action
DCWS-6028 (config-wireless)#network 1
DCWS-6028 (config-network)#mac authentication local!开启MAC本地认证
```

（2）拒绝无线终端接入列表。

```
DCWS-6028(config-wireless)#mac-authentication-mode black-list   !黑名单列表
DCWS-6028(config-wireless)#known-client 00-22-22-22-22-22 action
```

```
global-action
    DCWS-6028(config-wireless)#network 1
    DCWS-6028(config-network)#mac authentication local        !开启MAC本地认证
    DCWS-6028#wireless ap profile apply 1                     !下发配置生效
```

知识拓展

Client1、Client2 和 Client3 都通过 AP1 连接网络，如图 6-3-2 所示。

现假设 Client1 想与 Client3 连接，但不知道 Client3 的 MAC 地址。假如此时开启的 ARP 抑制模式为 ARP 代理，则 AP1 接到 Client1 的 ARP-Request 信号后，AP 会将映射表中 Client3 的 MAC 地址返回 ARP-Reply，而不必再将 ARP-Request 广播给所有的 Client。为了达到这样的目的，需要使用 ARP 代理功能并进行相应的配置。

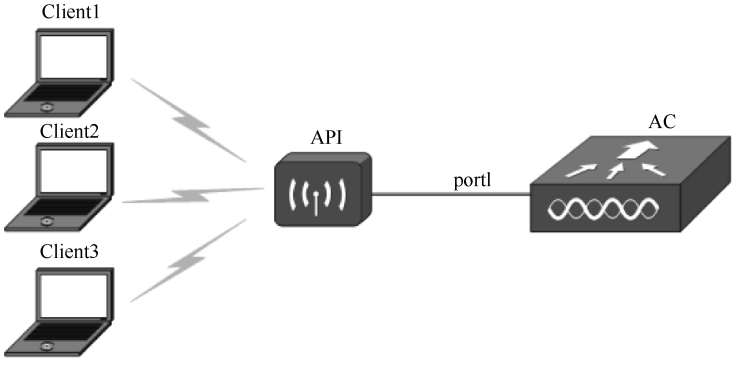


图 6-3-2　配置 ARP 抑制

相关命令如下。

```
DCWS-6028>enable
DCWS-6028#config
DCWS-6028(config)# wireless
DCWS-6028(config-wireless)# network 1
DCWS-6028(config-network)# arp-suppression
```

学习小结

本任务主要学习无线 AC 的安全控制，可以采取的安全策略包括动态黑名单、白名单、ARP 抑制等，使用这些方法可实现无线网络的安全办公。

项目考核

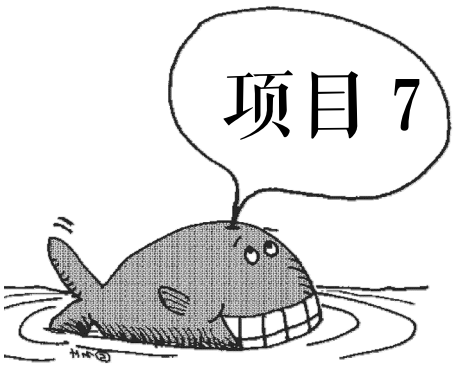
宏达公司无线网络要求配置两个 WLAN，SSID 分别为 teacher 和 student，采用 WPA2 加密方式，密钥为 11121314，如图 6-3-3 所示。

图 6-3-3　宏达公司拓扑结构

要求：

（1）实现无线用户二层隔离。

（2）限制用户上行带宽为 2Mb/s，下行带宽为 1Mb/s。



防火墙的配置

项目学习说明

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一种获取安全性方法的形象说法。它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关四个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

本项目重点学习防火墙的基本配置和防火墙的 VPN 实现。

学习能力目标

学习任务 1 防火墙的基本配置
学习任务 2 防火墙的 VPN 实现

职业能力目标

- 熟练掌握防火墙的初级管理
- 熟练掌握防火墙的典型环境安全策略
- 熟练掌握防火墙的 SSL VPN 的配置
- 熟练掌握防火墙的 IPSec VPN 的配置

学习任务 1　防火墙基本配置

防火墙系统是指设置在不同网络（如可信任的企业内部网和不可信任的公共网）或网络安全域之间的一系列部件的组合。它可通过监测、限制、更改跨越防火墙的数据流，尽可能

地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。在逻辑上，它是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。本学习任务分成以下两个学习活动进行。

学习活动 1　防火墙初级管理。

学习活动 2　防火墙典型环境安全策略实施。

学习活动 1　防火墙初级管理

防火墙的初级管理主要是熟悉防火墙各接口及其连接方法，熟练使用各种线缆实现防火墙与主机和交换机的连通，实现控制台连接防火墙进行初始配置，掌握防火墙管理环境的搭建和配置方法，熟练使用各种管理方式管理防火墙。

学习情境

公司规模不断扩大，经理为了提高网络的安全性，让网络管理员购买一个可以满足网络安全需求的设备，网络管理员认为、购买 DCFW-1800S-H-V2 防火墙可以实现公司的网络安全需求。

情境分析

防火墙是当今使用最为广泛的安全设备，防火墙历经几代发展，现今为非常成熟的硬件体系结构，具有专门的 Console 口、专门的区域接口。它串行部署于 TCP/IP 网络中。一般将网络划分为内、外、服务器区三个区域，对各区域实施安全策略以保护重要网络。

V2 防火墙可以使用 Telnet、SSH、WebUI 方式进行管理，使用者可以很方便地使用几种方式进行管理。本任务使用 DCFW-1800S-H-V2 防火墙。

所需设备如下。

（1）防火墙 DCFW-1800S-H-V2 设备 1 台。

（2）Console 线 1 条。

（3）网络线 2 条。

（4）PC 1 台。

防火墙初级管理如图 7-1-1 所示。

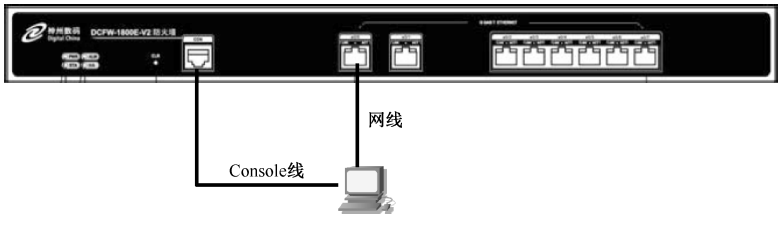


图 7-1-1　防火墙初级管理

相关知识

默认出厂时防火墙 E0/0 接口 IP 地址为 192.168.1.1/24，可将管理主机 IP 地址配置为

192.168.1.0/24 网段 IP 地址，与防火墙 E0/0 接口相连，通过 Web 登录防火墙管理界面。

在浏览器地址栏中输入以下两种 URL 均可：

```
http://192.168.1.1
https://192.168.1.1 ——  经过 SSL 加密，推荐使用
```

V2 防火墙默认的管理员是 admin，可以对其进行修改，但不能删除该管理员。增加一个管理员的命令如下：

```
DCFW-1800(config)#admin  user  user-name
```

执行该命令后，系统创建指定名称的管理员，并且进入管理员配置模式；如果指定的管理员名称已经存在，则直接进入管理员配置模式。

管理员特权为管理员登录设备后拥有的权限。DCFOS 允许的权限有 RX 和 RXW 两种。在管理员配置模式下，输入以下命令配置管理员的特权：

```
DCFW-1800(config-admin)#privilege {RX | RXW}
```

在管理员配置模式下，输入以下命令配置管理员的密码：

```
DCFW-1800(config-admin)#password password
!修改默认管理员 admin 口令
DCN(config)# admin user admin
DCN(config-admin)# password  q!Jiwx$*lc2H64cd#
!修改默认的管理服务端口
DCN(config)# http port 8088
DCN(config)# https port  1211
```

创建具有不同权限的管理员：

（1）需要使用 admin 账户创建新的管理员账户，并可对其进行修改、删除。

（2）使用 admin 添加的新管理员账户可赋予不同的权限（读、写）。

（3）使用 admin 添加的新管理员账户可赋予不同的管理方式（Console、Telnet、SSH、HTTP、HTTPS）。

步骤实现

1. 初步认识防火墙

步骤 1：认识防火墙各接口，理解防火墙各接口的作用，并学会使用线缆连接防火墙和交换机与主机，如图 7-1-2 所示。

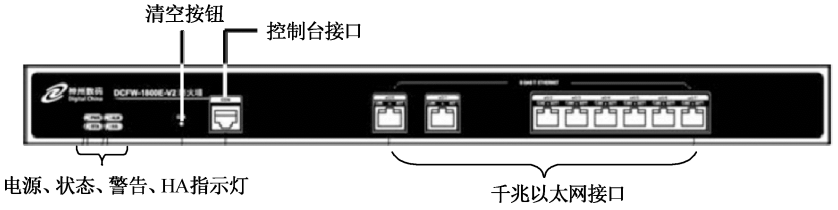


图 7-1-2　初步认识防火墙

步骤 2：使用 Console 线缆将防火墙与 PC 的串行接口连接起来，如图 7-1-3 所示。

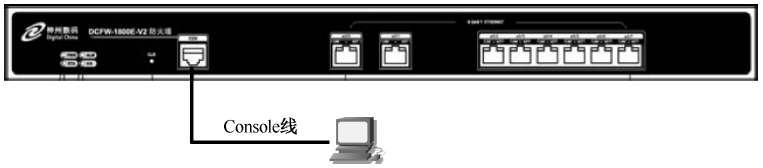


图 7-1-3　防火墙与 PC 连接

步骤 3：配置 PC 的超级终端属性，接入防火墙命令行模式，登录防火墙并熟悉各配置模式。默认管理员用户口令和密码如下：

```
login：admin
password：admin
```

输入如上信息，可进入防火墙的执行模式，该模式的提示符包含了一个数字符号（#）：

```
DCFW-1800#
```

在执行模式下，输入 configure 命令，可进入全局配置模式：

```
DCFW-1800(config)#
```

V2 系列防火墙的不同模块功能需要在其对应的命令行子模块模式下进行配置。在全局配置模式中输入特定的命令可以进入相应的子模块配置模式。例如，运行 interface ethernet0/0 命令进入 E0/0 接口配置模式，此时的提示符变更为

```
DCFW-1800(config-if-eth0/0)#
```

步骤 4：通过 PC 测试与防火墙的连通性。

使用交叉线连接防火墙和 PC，此时防火墙的 LAN-link 灯亮起，表明网络的物理连接已经建立。观察指示灯状态为闪烁，表明有数据在尝试传输。

此时打开 PC 的连接状态，发现只有数据发送，没有接收到数据，这是因为防火墙的端口默认状态下会禁止向未经验证和配置的设备发送数据，以保证数据的安全。

2. 搭建 Telnet 和 SSH 管理环境

步骤 1：运行 manage telnet 命令，开启被连接接口的 Telnet 管理功能。

```
Hostname#configure
DCFW-1800(config)#interface Ethernet 0/0
DCFW-1800(config-if-eth0/0)#manage telnet
```

步骤 2：运行 manage ssh 命令，开启 SSH 管理功能。

```
DCFW-1800(config-if-eth0/0)#manage ssh
```

步骤 3：配置 PC 的 IP 地址为 192.168.1.*，从 PC 上尝试与防火墙的 Telnet 进行连接。注意：用户口令和密码是默认管理员用户口令和密码，即均为 admin，如图 7-1-4 和图 7-1-5 所示。

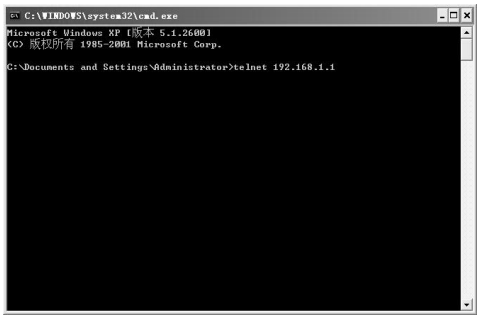


图 7-1-4　Telnet 防火墙界面

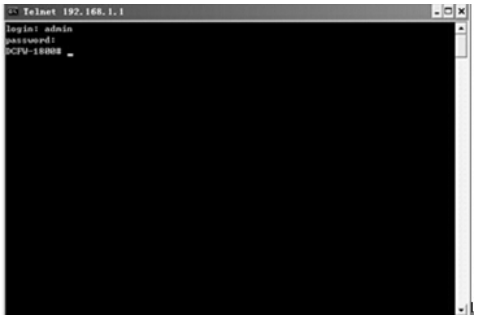


图 7-1-5　输入用户名和密码后连接成功

3．搭建 WebUI 管理环境

步骤 1：初次使用防火墙时，用户可以通过 E0/0 接口访问防火墙的 WebUI 页面。在浏览器地址栏中输入“ https://192.168.1.1 ”并按【Enter】键，系统 WebUI 的登录界面如图 7-1-6 所示。

图 7-1-6　防火墙 Web 登录界面

步骤 2：登录后的主界面如图 7-1-7 所示。

图 7-1-7　登录成功后的主界面

学习小结

本学习活动介绍了防火墙的初级管理，需要注意的是管理方式有 Console 口、Telnet、HTTP 等，但初始化的防火墙一般使用 HTTP 方式，如想实现 Telnet 方式的管理，只要进行相关的配置，但 HTTP 管理方式更容易掌握。

学习活动 2　防火墙典型环境安全策略实施

学习情境

公司为了保证内部网络的安全性，购买了防火墙，考虑到公网地址有限，为了节约成本，不能每台 PC 都配置公网地址访问外网。于是管理员想使用防火墙的混合模式来实现联网，通过少量公网 IP 地址来满足多数私网 IP 地址联网，以缓解 IP 地址不足并节约公司成本。

情境分析

混合模式相当于防火墙既工作于路由模式，又工作于透明模式。在实际应用环境中，此类防火墙应用一般也比较广泛。混合模式分为两种。第一种是 ISP 分配内网地址，内网为私网地址，服务器区域和内部地址为同一网段。这样，内部区域和服务器区域为透明，内部区域和外网区域为路由，服务器区域和外部区域也为路由。第二种是 ISP 分配外网地址，内网为私网地址，服务器区域使用 ISP 分配的公网地址，服务器区域和外网为透明，内部区域和外部区域为路由。在下面的应用环境中我们使用的是第二种混合模式。

所需设备：

（1）防火墙设备 1 台。

（2）Console 线 1 条。

（3）网络线 2 条。

（4）PC 1 台。

公司网络拓扑结构如图 7-1-8 所示。

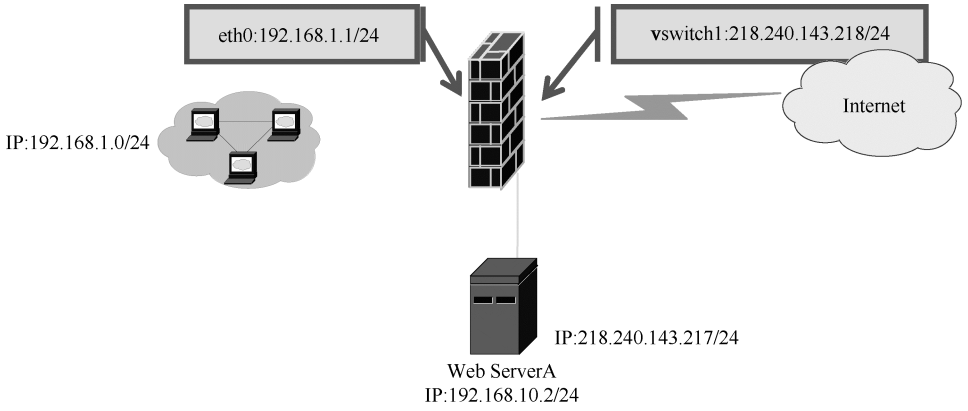


图 7-1-8　公司网络拓扑结构

步骤实现

步骤 1：设置内网口地址，设置 eth0 接口为内网口地址，即 192.168.1.1/24，如图 7-1-9 所示。

图 7-1-9　设置内网口地址

步骤 2：设置外网口，eth6 接口连接外网，将 eth6 接口设置成二层安全域 l2-untrust，如图 7-1-10 所示。

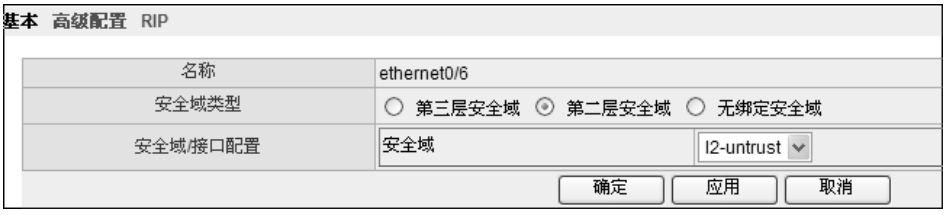


图 7-1-10　设置外网口

步骤 3：设置服务器接口，将 eth7 接口设置成 l2-dmz 安全域，连接服务器，如图 7-1-11 所示。

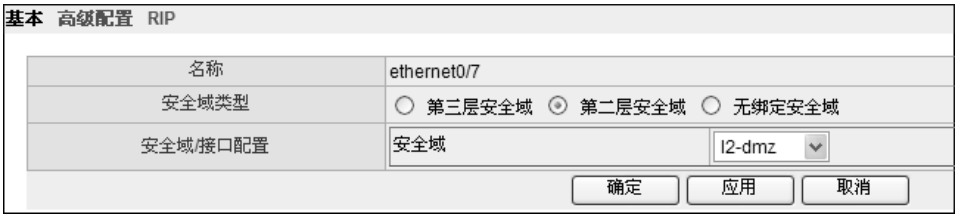


图 7-1-11　设置服务器接口

步骤 4：配置 vswitch 接口。由于二层安全域接口不能设置地址，因此需要将地址设置在网桥接口上，该网桥接口即为 vswitch，如图 7-1-12 所示。

图 7-1-12　配置 vswitch 接口

步骤 5：设置 SNAT 策略。针对内网所有地址我们在防火墙上设置源 NAT，内网 PC 在访问外网时，凡是从 vswitch 接口出去的数据包都做地址转换，转换地址为 vswitch 接口地址，

如图 7-1-13 所示。

图 7-1-13　设置 SNAT 策略

步骤 6：添加路由。要创建一条到外网的默认路由，如果内网有三层交换机，则需要创建到内网的回指路由，如图 7-1-14 所示。

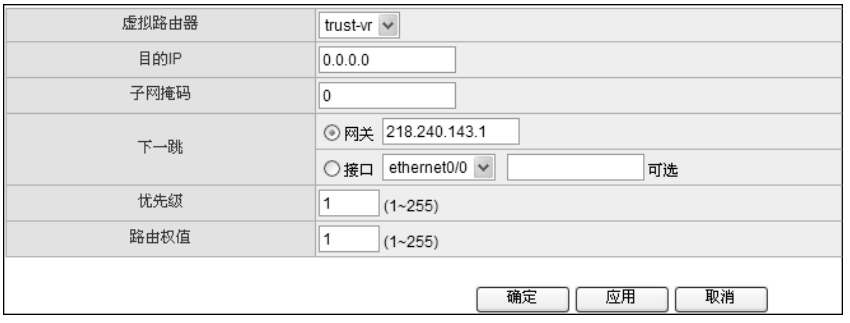


图 7-1-14　添加路由

步骤 7：设置地址簿。在放行安全策略时，需要选择相应的地址和服务进行放行，这里首先要创建服务器的地址簿。在创建地址簿时，如果创建的服务器属于单个 IP，使用 IP 成员方式，则子网掩码一定要写 32 位，如图 7-1-15 所示。

图 7-1-15　设置地址簿

步骤 8：放行策略。放行策略时，首先要保证内网能够访问到外网。应该放行内网口所属安全域到 vswitch 接口所属安全域的安全策略，即从 trust 到 untrust，如图 7-1-16 所示。

步骤 9：要保证外网能够访问 Web_server，该服务器的网关地址设置为 ISP 的网关 218.240.143.1。需要在放行二层安全之前设置安全策略，应该放行 l2-untrust 到 l2-dmz 策略。

图 7-1-16　设置放行策略

小贴士

如果服务器的网关并没有设置成 218.240.143.1，而设置成 vswitch 的接口地址，此时安全策略如何设置才能让外网访问到 Web 服务器？

按上述实验配置完后，在外网可以访问服务器，那么在服务器上是否可以访问外网呢？如果访问不到是什么原因，如何才能实现访问？

学习小结

本学习活动介绍了防火墙的典型环境安全策略实施，需要注意路由模式和透明模式的区别。

学习任务 2　实现防火墙上的 VPN 技术

如今大多数的防火墙支持 VPN 技术，这样可以大大节省公司的资金，从而使得公司的内部网络更加安全和方便。本学习任务分成以下两个学习活动进行。

学习活动 1　实现防火墙的 SSL VPN 技术。

学习活动 2　实现防火墙 IPSec VPN 技术。

学习活动 1　实现防火墙的 SSL VPN 技术

SSL VPN 属于远程登录。例如，访问公司内网，需要先连接 SSL VPN 然后访问公司或者企业内部网络。SSL VPN 可以作为加密通道，保障数据安全。

学习情境

公司的员工经常出差，在外地的时候经常需要访问公司的服务器，但总是不太安全，网

络管理员想通过防火墙的 VPN 来实现此访问。基于公司的现状，网络管理员决定使用 SSL VPN 来实现此功能。

情境分析

为解决远程用户安全访问私网数据的问题，DCFW-1800 系列防火墙提供了基于 SSL 的远程登录解决方案。SSL VPN 可以通过简单易用的方法实现信息的远程连通。防火墙的 SSL VPN 功能包含设备端和客户端两部分，配置了 SSL VPN 功能的防火墙作为设备端。外网用户通过 Internet 使用 SSL VPN 接入内网。所以网络管理员的决定是正确的。

所需设备：

（1）防火墙设备 1 台。

（2）局域网交换机若干台。

（3）网络线若干条。

（4）PC 若干台。

防火墙 SSL VPN 拓扑结构如图 7-2-1 所示。

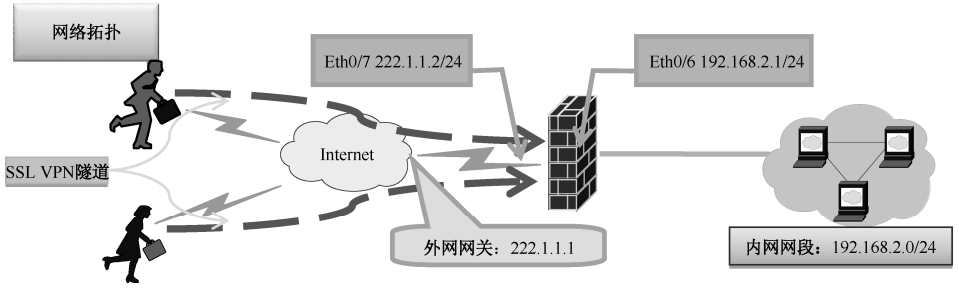


图 7-2-1　防火墙 SSL VPN 拓扑结构

相关知识

SSL VPN 指的是基于安全套接层协议（Security Socket Layer，SSL）建立远程安全访问通道的 VPN 技术。它是近年来兴起的 VPN 技术，其应用随着 Web 的普及和电子商务、远程办公的兴起而迅速发展。

SSL VPN 由于其强大的功能和实施的方便性应用越来越广泛，市场上的 SSL VPN 品牌也越来越多，如何选择适合自己的产品是需要用户仔细考虑的一个问题。

SSL VPN 的发展迎合了用户对低成本、高性价比远程访问的需求。现在，它已经广泛应用于各行各业。选购 SSL VPN 时，用户要根据自身特点和不同的业务模式，选择适合自己的 SSL VPN 产品。再次强调，VPN 是正在发展的技术，更新换代可能会比较快，因此用户在选购时可以少考虑一些扩展性，多注重产品的实用性。毕竟，只有适合自己的，才是最理想的选择。

SSL 协议主要是由 SSL 记录协议和握手协议组成的。它们共同为应用访问连接提供认证、加密和防篡改功能。SSL 握手协议相对于 IPSec 协议体系中的 IKE（互联网密钥交换协议）协议而言，主要用于服务器和客户之间的相互认证，协商加密算法和 MAC（Message Authentication Code，消息认证码）算法，用于生成在 SSL 记录协议中使用的加密和认证密

钥。SSL 记录协议为各种应用协议提供基本的安全服务，类似于 IPSec 的传输模式，应用程序消息参照 MTU（最大传输单元）被分割成可治理的数据块（可进行数据压缩处理），并产生一个 MAC 信息，加密后插入新的报头，最后在 TCP 中加以传输；接收端将收到的数据解密，做身份验证（MAC 认证）、解压缩、重组数据报然后交给应用协议进行处理。实际上就是在应用层和传输层之间加入了一个数据处理层，和传统的网络套接字模型在同一层次，这也就是安全套接层的由来。

步骤实现

步骤 1：配置 SCVPN 地址池，在“ VPN ”→“ SCVPN ”→“ 地址池 ”中新建一个名为 scvpn_pool1 的地址池，如图 7-2-2 所示。

图 7-2-2　配置 SCVPN 地址池

步骤 2：配置 SCVPN 实例，在“ VPN ”→“ SCVPN ”→“ 配置 ”中，创建一个 SCVPN 实例，定义 SCVPN 接入使用的各种参数，如图 7-2-3 所示。

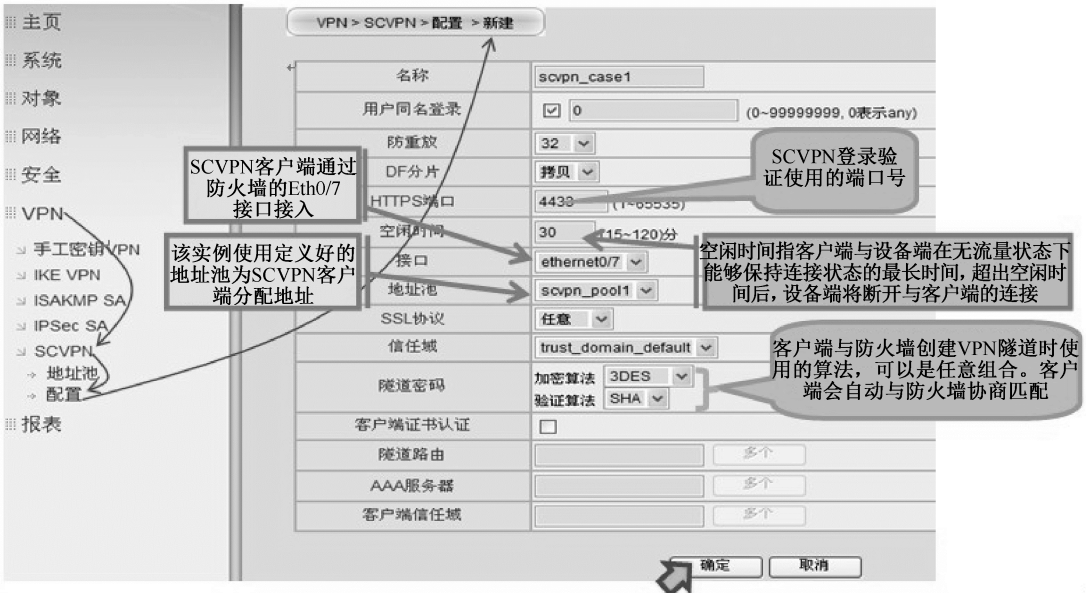


图 7-2-3　配置 SCVPN 实例

步骤 3：创建完 SCVPN 实例并编辑完成各种参数后，还需要对该实例重新编辑。单击已

编辑好的实例中的“ 修改 ”按钮，如图 7-2-4 所示。

图 7-2-4　查看实例配置参数

步骤 4：添加隧道路由条目。在客户端与防火墙的 SCVPN 创建成功后会下发到客户端的路由表中。添加的网段就是客户端要通过 VPN 隧道访问的位于防火墙内网的网段。需要注意的是，此处添加的路由条目的“ 度量 ”值比客户端上默认路由的度量值小。度量值越小的路由条目优先级越高，如图 7-2-5 所示。

图 7-2-5　添加隧道路由条目

步骤 5：将 Web Server 的隧道路由下发到客户端，如图 7-2-6 所示。

图 7-2-6　Web Server 的隧道路由下发到客户端

步骤 6：添加的 AAA 服务器是用来验证客户端登录的用户名、密码的。目前防火墙支持的验证方式有四种：防火墙本地验证、RADIUS 验证、Active-Directory 验证和 LDAP 验证，如图 7-2-7 所示。

图 7-2-7　添加的 AAA 服务器

步骤 7：创建 SCVPN 所属安全域，在“网络”→“安全域”中为创建的 SCVPN 新建一个安全域，安全域类型为“第三层安全域”，如图 7-2-8 所示。

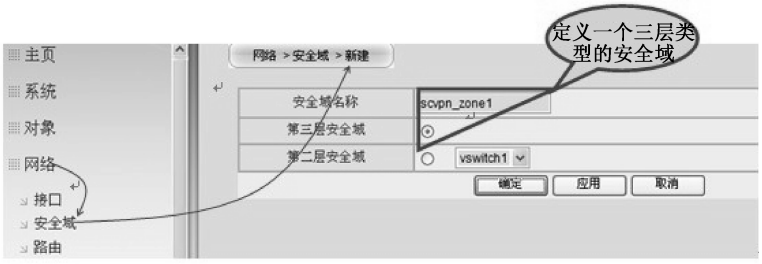


图 7-2-8　创建 SCVPN 所属安全域

步骤 8：创建隧道接口并引用 SCVPN 隧道。为了 SCVPN 客户端能与防火墙上其他接口所属区域之间正常路由转发，需要为它们配置一个网关接口，这在防火墙上通过创建一个隧道接口，并将创建好的 SCVPN 实例绑定到该接口上来实现，如图 7-2-9 所示。

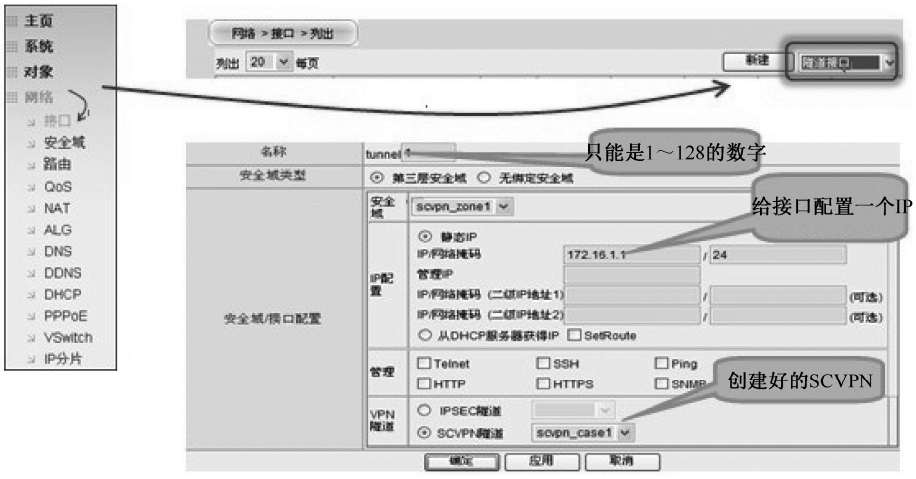


图 7-2-9　创建隧道接口并引用 SCVPN 隧道

步骤 9：创建安全策略。在放行安全策略前，首先要创建地址簿和服务簿。为创建 SCVPN 客户端访问内网 Server 的安全策略，要将策略中引用的对象定义好，如图 7-2-10 所示。

图 7-2-10　定义 FTP Server 的地址对象

步骤 10：定义 Web Server 的地址对象。添加安全策略，以允许 SCVPN 用户访问内网资源，添加策略 1 允许 SCVPN 用户访问内网 FTP Server，仅开放 FTP 服务。添加策略 2，允许 SCVPN 用户访问内网 Web Server，仅开放 HTTP 服务，如图 7-2-11 所示。

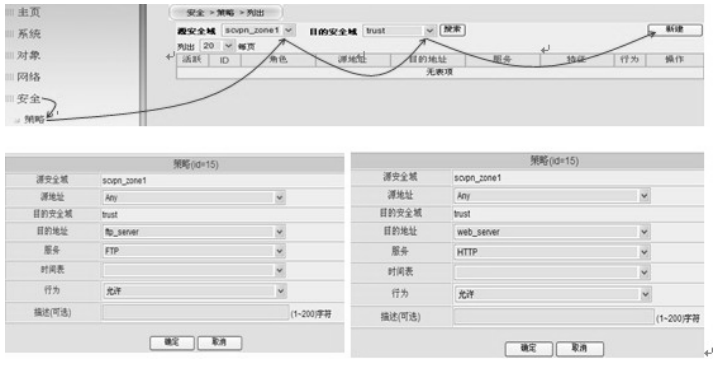


图 7-2-11　定义 Web Server 的地址对象

步骤 11：添加 SCVPN 用户账号，如图 7-2-12 所示。

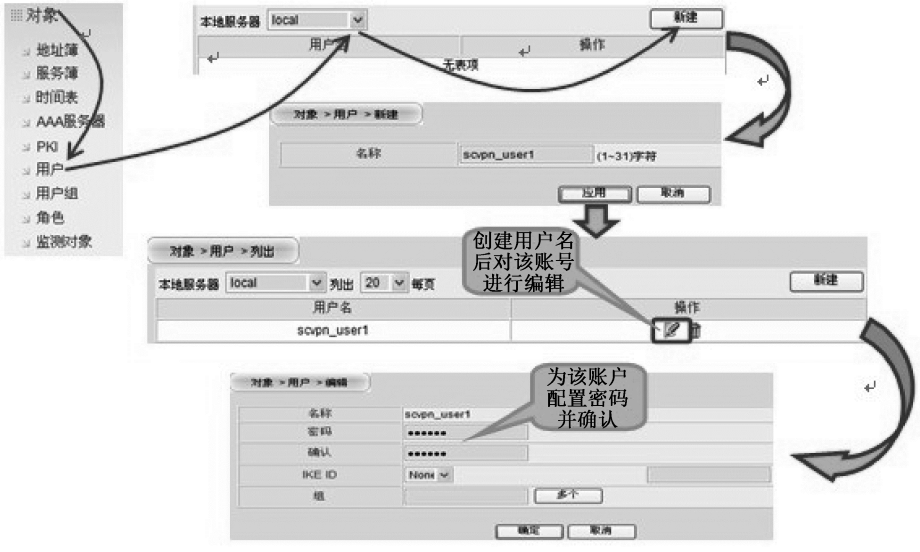


图 7-2-12　添加 SCVPN 用户账号

步骤 12：SCVPN 登录演示。在客户端上打开浏览器，在地址栏中键入“ https://222.1.1.2:4433 ”，在登录界面中填入用户账号和密码，单击“ 登录 ”按钮，如图 7-2-13 所示。

图 7-2-13　登录界面

步骤 13：在初次登录时，会要求安装 SCVPN 客户端插件，此插件以 ActiveX 插件方式推送下载，并有可能被浏览器拦截，这时需要手动允许安装这个插件，如图 7-2-14 所示。

图 7-2-14　安装插件

步骤 14：SCVPN 客户端的安装，对下载完成的客户端安装程序进行手动安装，如图 7-2-15 所示。

图 7-2-15　安装客户端软件

步骤 15：SCVPN 客户端安装成功后会登录防火墙，在对用户名和密码验证成功后，任务栏右下角的客户端程序图标会变成绿色，并在 Web 界面中显示 “ 连接成功 ”，如图 7-2-16 所示。

图 7-2-16　连接成功界面

步骤 16：单击任务栏中的客户端程序图标，在弹出的菜单中执行“ Network Information ”命令，即可查看连接信息，如图 7-2-17 所示。

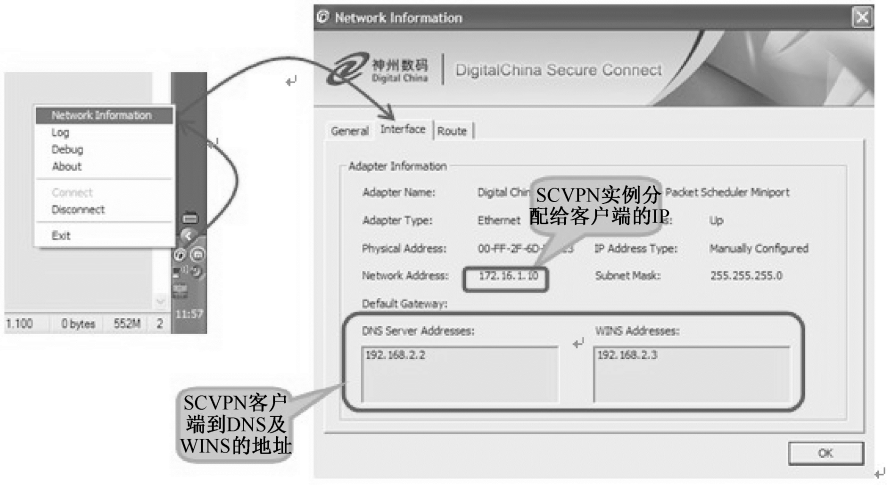


图 7-2-17　查看连接信息

步骤 17：在客户端的“ Route ”选项卡中查看下发给客户端的路由信息，如图 7-2-18 所示。

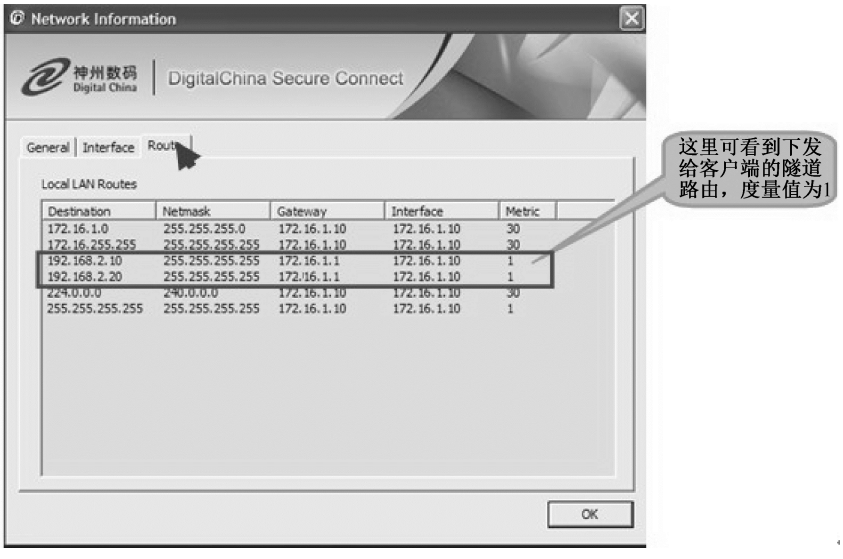


图 7-2-18　查看路由信息

小贴士

可以设置几个不同权限的角色，不同的账号所属的角色不同，这样不同的账号登录认证成功后，其放行的服务不同或所具有的权限不同。

学习小结

本学习活动介绍了防火墙的 SCVPN 技术，这种技术针对最终用户的 PC 和便携式计算机需要装入客户软件，使得用户出差访问公司内部网络更加安全。 SCVPN 还可以降低部署成本、减小对日常性支持和管理的需求。

学习活动 2　实现防火墙 IPSec VPN 技术

IPSec VPN 即指采用 IPSec 协议来实现远程接入的一种 VPN 技术, IPSec 是由 IETF 定义的安全标准框架，用以提供公用和专用网络的端对端加密和验证服务。IPSec 协议通过包封装技术，能够利用 Internet 可路由的地址，封装内部网络的 IP 地址，实现异地网络的互通。

学习情境

由于规模的扩大，总公司和分公司之间都购买了防火墙，出于安全性考虑，网络管理员想在两个防火墙之间使用一种更安全的 VPN 连接方式, 网络管理员认为防火墙的 IPSec VPN 可以实现此功能。

情境分析

IPSec VPN 是现在互联网上最重要的网关到网关 VPN 技术, 它已经成为企业分支机构间互连的首选技术。总部和分支之间要实现互访时，就涉及此类 VPN，或者需要对数据包进行加密时就涉及 IPSec VPN。

所需设备：

（1）防火墙设备 2 台。

（2）局域网交换机若干台。

（3）网络线若干条。

（4）PC 若干台。

防火墙 IPSec VPN 如图 7-2-19 所示。

防火墙 FW-A 和 FW-B 都具有合法的静态 IP 地址, 其中防火墙 FW-A 的内部保护子网为 192.168.1.0/24，防火墙 FW-B 的内部保护子网为 192.168.10.0/24。要求在 FW-A 与 FW-B 之间创建 IPSec VPN，使两端的保护子网能通过 VPN 隧道互相访问。

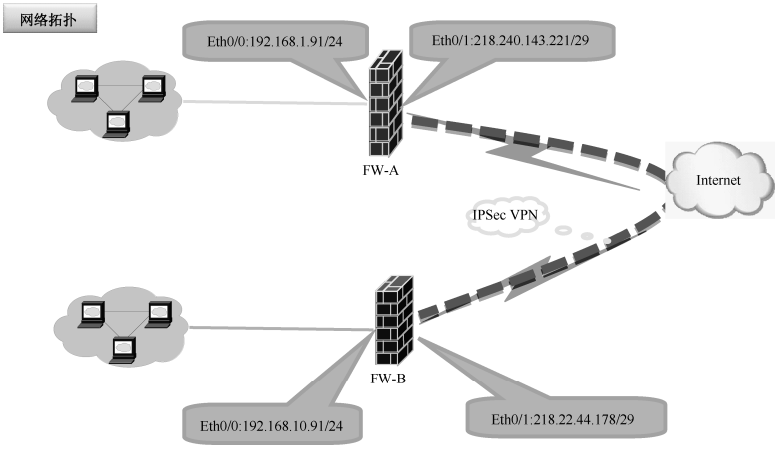


图 7-2-19　防火墙 IPSec VPN

相关知识

创建防火墙 IPSec VPN 的步骤如下。

（1）创建 IKE 第一阶段提议。

（2）创建 IKE 第二阶段提议。

（3）创建对等体（peer）。

（4）创建隧道。

（5）创建隧道接口，并将创建好的隧道绑定到接口。

（6）添加隧道路由。

（7）添加安全策略。

步骤实现

步骤 1：创建 IKE 第一阶段提议，在“ VPN ”→“ IKE VPN ”→“ P1 提议 ”中定义 IKE 第一阶段的提议内容，两台防火墙的 IKE 第一阶段提议内容需要一致，如图 7-2-20 所示。

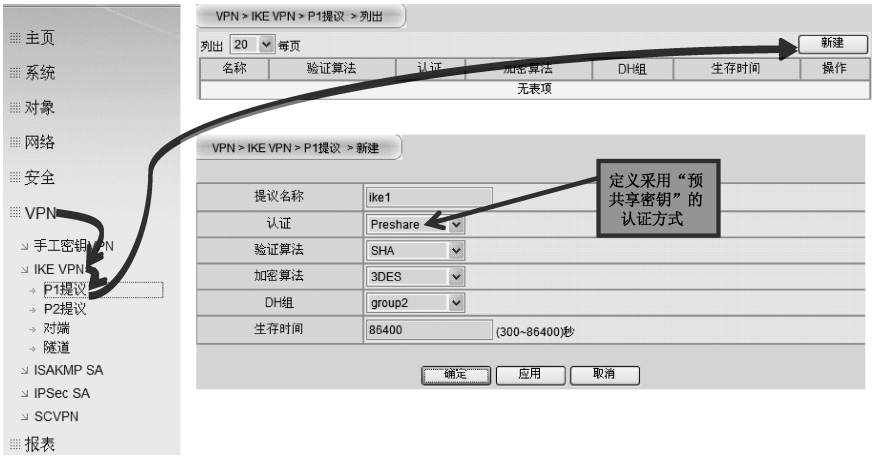


图 7-2-20　创建 IKE 第一阶段提议

步骤 2：创建 IKE 第二阶段提议，在“ VPN ”→“ IKE VPN ”→“ P2 提议 ”中定义 IKE 第二阶段的提议内容，两台防火墙的第二阶段提议内容需要一致，如图 7-2-21 所示。

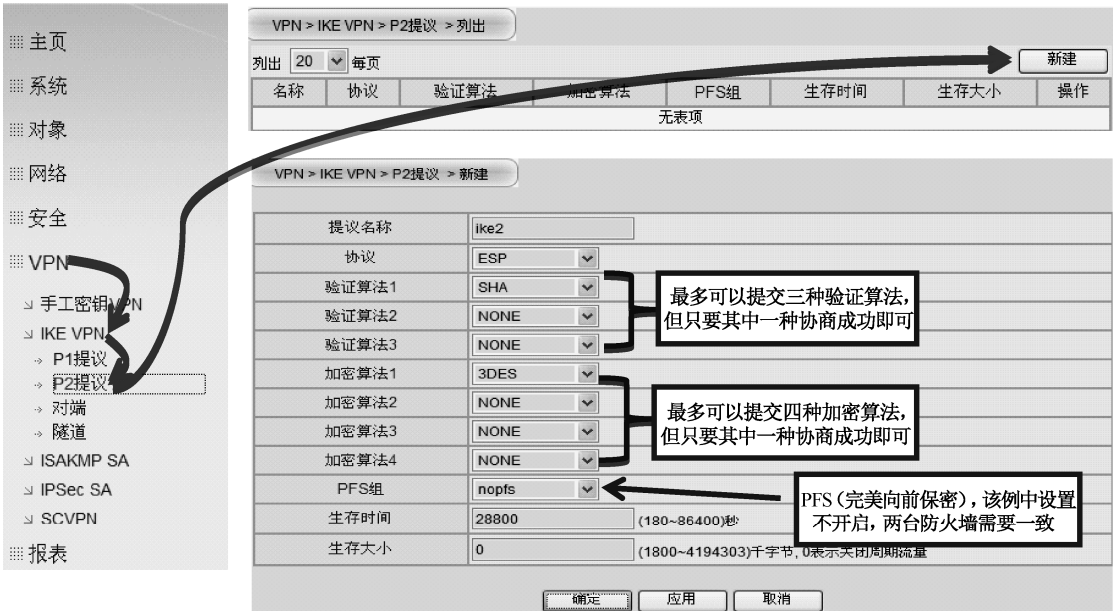


图 7-2-21　创建 IKE 第二阶段提议

步骤 3：创建对等体。在“ VPN ”→“ IKE VPN ”→“ 对端 ”中创建“ 对等体 ”对象，并定义对等体的相关参数，如图 7-2-22 所示。

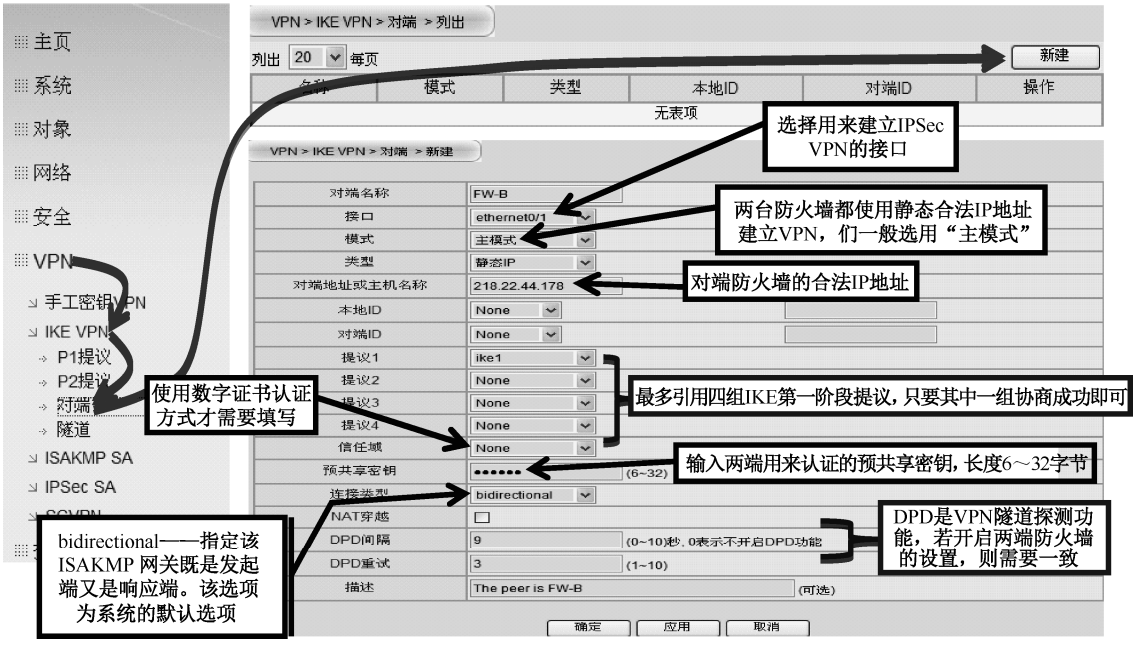


图 7-2-22　创建对等体

步骤 4：创建隧道。在“ VPN ”→“ IKE VPN ”→“ 隧道 ”中创建到防火墙 FW-B 的 VPN 隧道，并定义相关参数，如图 7-2-23 所示。

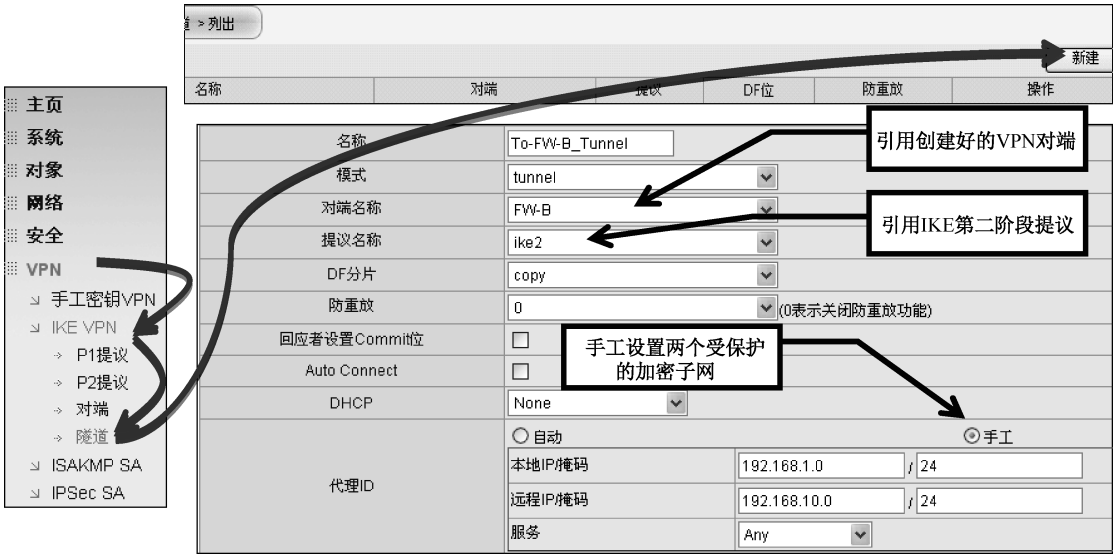


图 7-2-23　创建隧道

步骤 5：创建隧道接口并与 IPSec 绑定。在“ 网络 ”→“ 接口 ”中新建隧道接口，指定安全域并引用 IPSec 隧道，如图 7-2-24 所示。

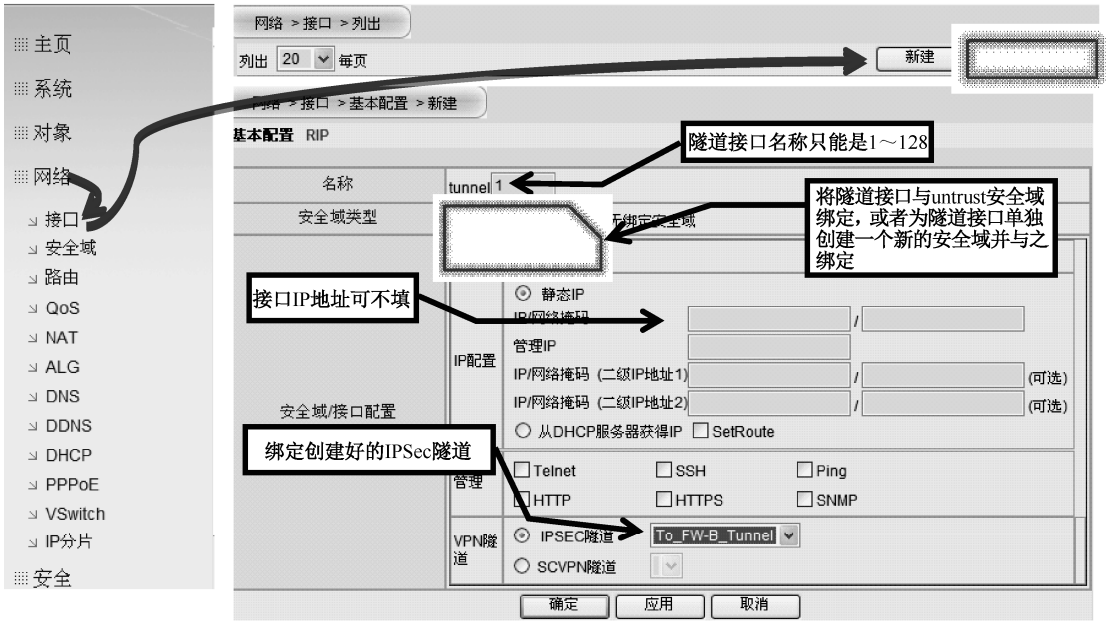


图 7-2-24　创建隧道接口并与 IPSec 绑定

步骤 6：添加隧道路由。在“ 网络 ”→“ 路由 ”→“ 目的路由 ”中新建一条路由，目的地址是对端加密保护子网，网关为创建的 tunnel 接口，如图 7-2-25 所示。

步骤 7：添加安全策略。在创建安全策略前先要创建本地网段和对端网段的地址簿，如图 7-2-26 和图 7-2-27 所示。

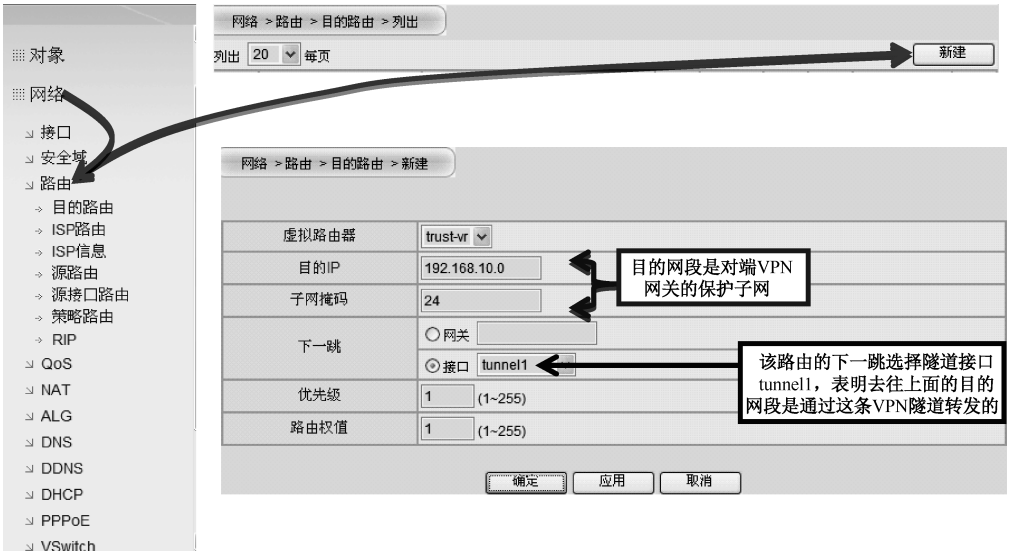


图 7-2-25　添加隧道路由

图 7-2-26　添加地址簿

图 7-2-27　添加地址成员

步骤 8：成功创建两个地址簿后，在“安全”→“策略”中新建策略，允许本地 VPN 保护子网访问对端 VPN 保护子网，如图 7-2-28 所示。

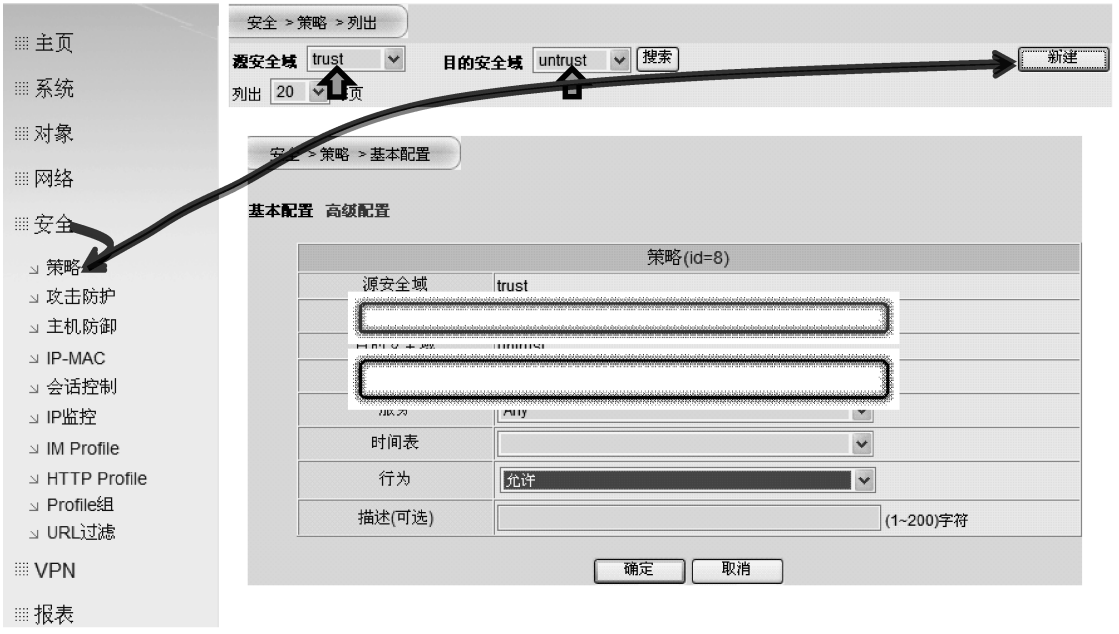


图 7-2-28　添加策略

步骤 9：允许对端 VPN 保护子网访问本地 VPN 保护子网，如图 7-2-29 所示。

图 7-2-29　保护子网

步骤 10：FW-B 防火墙的配置步骤与 FW-A 相同，不同的只是某些步骤中的参数设置，此处略。

步骤 11：验证测试，查看防火墙 FW-A 上的 IPSec VPN 状态，如图 7-2-30 所示。

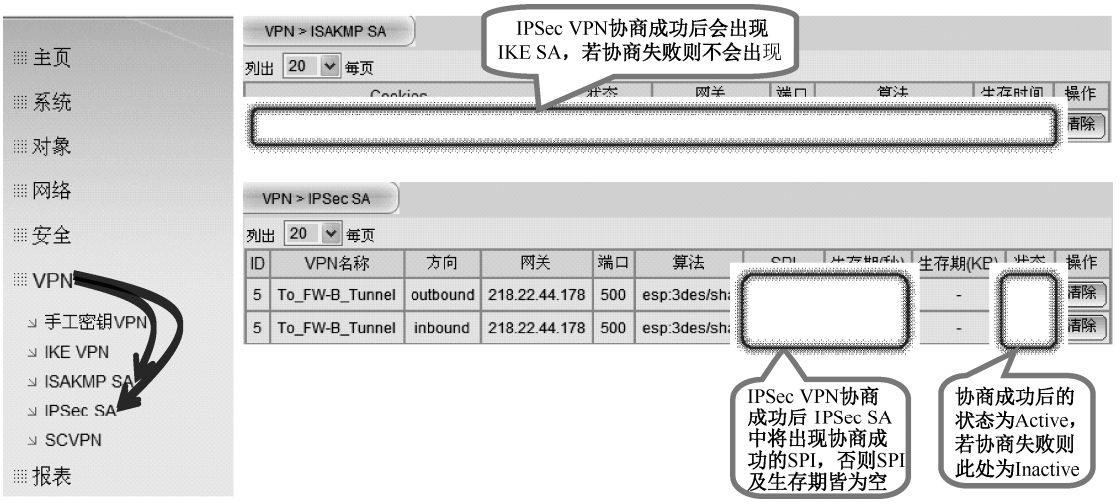


图 7-2-30　查看 FW-A 的状态

步骤 12：查看防火墙 FW-A 上的 IPSec VPN 状态，如图 7-2-31 所示。

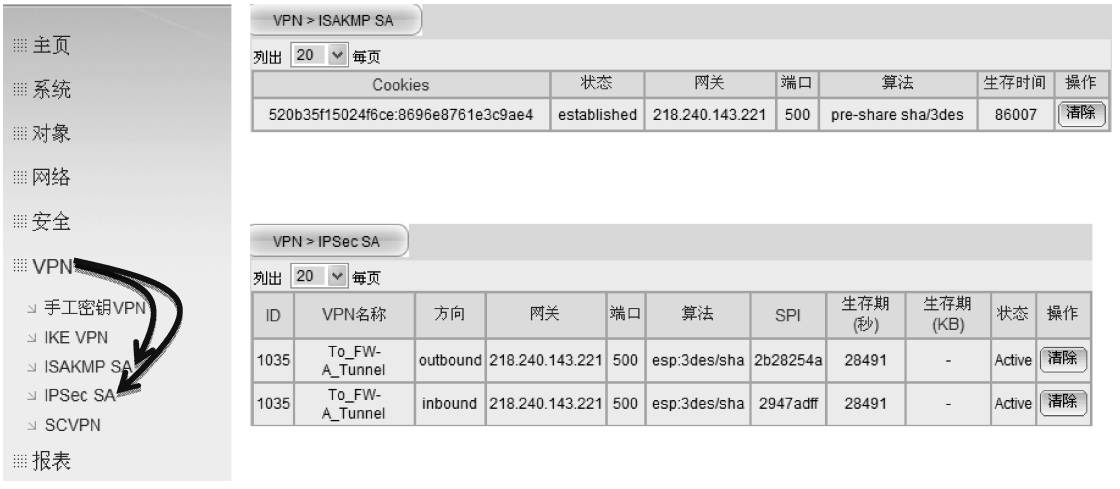


图 7-2-31　查看 FW-A 的 IPSec VPN 状态

学习小结

本学习任务介绍了防火墙的 IPSec VPN 技术，这种技术是一套具有比较完整体系的技术，它规定了一系列协议标准，在学习时要注意实现过程的步骤。

项目考核

1．防火墙 VPN 的实现。

假设你是公司的网络管理员，公司因业务扩大，建立了一个分公司，公司的业务数据很

重要，公司总部与分公司传输数据时需要加密，采用 IPSec VPN 技术对数据进行加密。总公司要加密的子网为 10.1.1.0/24，子公司要加密的子网为 10.1.2.0/24。

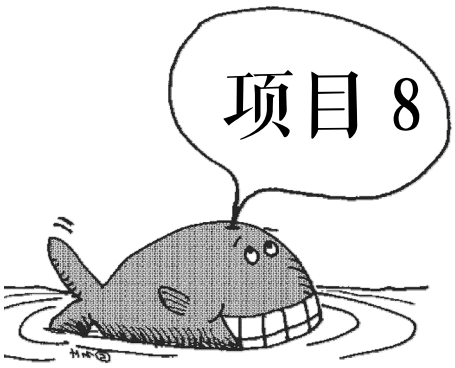
2．自己动手搭建网络环境，实现如下要求。

（1）在防火墙上创建 ninternet 区域、winternet 区域。

（2）只允许总部用户在上班时间（9:00～17:30）访问外网。

（3）不允许总部用户访问 360.com，用户访问网页时过滤掉 360，只能出现在网页中三次。

（4）为了让公司员工出差方便，在防火墙中建立一个 L2TP，使出差用户可以拨号访问总部资源。



综 合 实 战

项目学习说明

本项目重点针对网络设备的综合应用分任务进行讲述，主要为学习网络课程的初学者设计、配置、排除网络故障提供了良好的案例，让初学者更加熟悉网络设备的配置和在实际企业中的综合应用。

学习能力目标

学习任务 1　小型企业的网络工程案例
学习任务 2　企业网络综合实战

职业能力目标

- 能完成小型企业的网络设备配置。
- 能综合运用网络设备的相关技术实现企业的需求。

学习任务 1　小型企业的网络工程案例

本任务不但能将前几个项目所学的基本知识进行巩固，使学生熟练掌握前面项目所学的知识，而且能进一步学习到一些网络设备配置方面更高层次的应用，以及 VPN 等知识的应用。

学习情境

某科技型公司总部设在广州，由于业务发展的需要，准备在深圳设置分公司，为了实现快捷的信息交流和资源共享，需要构建一个跨地域的公司网络。总公司有销售部和管理部两个部门，分公司设有销售部。

总公司采用双核心交换机的网络架构，独立公共服务网络部分，确保内部网络安全。

为了实现快捷的信息传递和公司业务的需求，允许分公司办公的员工能够方便、快捷、安全地访问总公司内网服务器群。

外网采用 OSPF 动态路由协议，总公司内部和分公司内部采用私有地址和 RIPv2 协议，内部访问外部采用 NAT 协议。

情境分析

1. 网络连接

根据需求分析的描述与下列详细要求完成网络结构的设计与设备的连接，画出完整的网络拓扑结构图。拓扑结构图中需要明确列出设备接线的端口号，以及端口相关的 IP 地址。实际接线与设置必须按照拓扑结构图进行。

完成网络的规划设计后，请按以下要求进行网络的连接与配置。

（1）总公司使用一台路由器的网络出口接入互联网，总公司内部访问外部采用 NAT 协议，PC7 模拟互联网上的计算机。

（2）总公司的路由器分别下连两台三层交换机作为汇聚交换机，分别通过三层互连；两台三层汇聚交换机之间通过两条线路进行链路汇聚通信，另外一条线路作为链路备份，两台汇聚交换机下连两台接入交换机，并形成冗余链路，实现对客户的透明传输。

（3）总公司内部的路由器和汇聚交换机之间使用 RIPv2 路由协议，实现内部网络的互相通信。

（4）Switch-C 位于 9 楼办公室，Switch-D 位于 10 楼办公室，分别接有不同部门的员工机器。

（5）PC1 和 PC2 接入二层交换机 Switch-C，PC3 和 PC4 接入二层交换机 Switch-D；PC1 和 PC3 属于一个部门，划归 VLAN10，PC2 和 PC4 属于一个部门，划归 VLAN20。

（6）PC1～PC4 通过汇聚交换机 Switch-B 自动获取 IP 地址。

（7）分公司与公网之间使用 PPP 协议进行连接。

（8）分公司使用一台路由器的网络出口接入互联网，分公司使用一台路由器与运营商路由器通过 VPN（IPSec）技术互连。

（9）分公司的路由器下连一台二层交换机作为接入交换机，接入交换机下连两个部门的员工机器。

（10）PC5 和 PC6 接入二层交换机 Switch-E，PC5 属于一个部门，划归 VLAN70；PC6 属于一个部门，划归 VLAN80。

（11）PC5 和 PC6 通过公网的 Router-B 获取 IP 地址，且 PC5 和 PC6 可以相互通信。

（12）总公司、分公司与公网的外网之间使用 OSPF 路由协议，实现内部和外部网络的互相通信。

（13）根据设计估算所需要的耗材数量，准备好领料清单。

（14）根据上述要求完成拓扑设计后，制作线缆完成设备的连接。

（15）打配的跳线使用 T568B 线序，制作的线缆必须稳固耐用。

根据设计要求，网络互连的拓扑结构如图 8-1-1 所示，请按图中要求完成相关网络设备的连接。

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）DCS-3950 交换机 3 台。

（3）DCR-2626 路由器 3 台。

（4）模拟服务器的计算机 2 台。

（5）PC 7 台。

（6）直连和交叉双绞线若干条。

（7）Console 线 2 条。

（8）CR-V35MT　2 条。

（9）CR-V35FC　2 条。

网络互连的拓扑结构如图 8-1-1 所示。

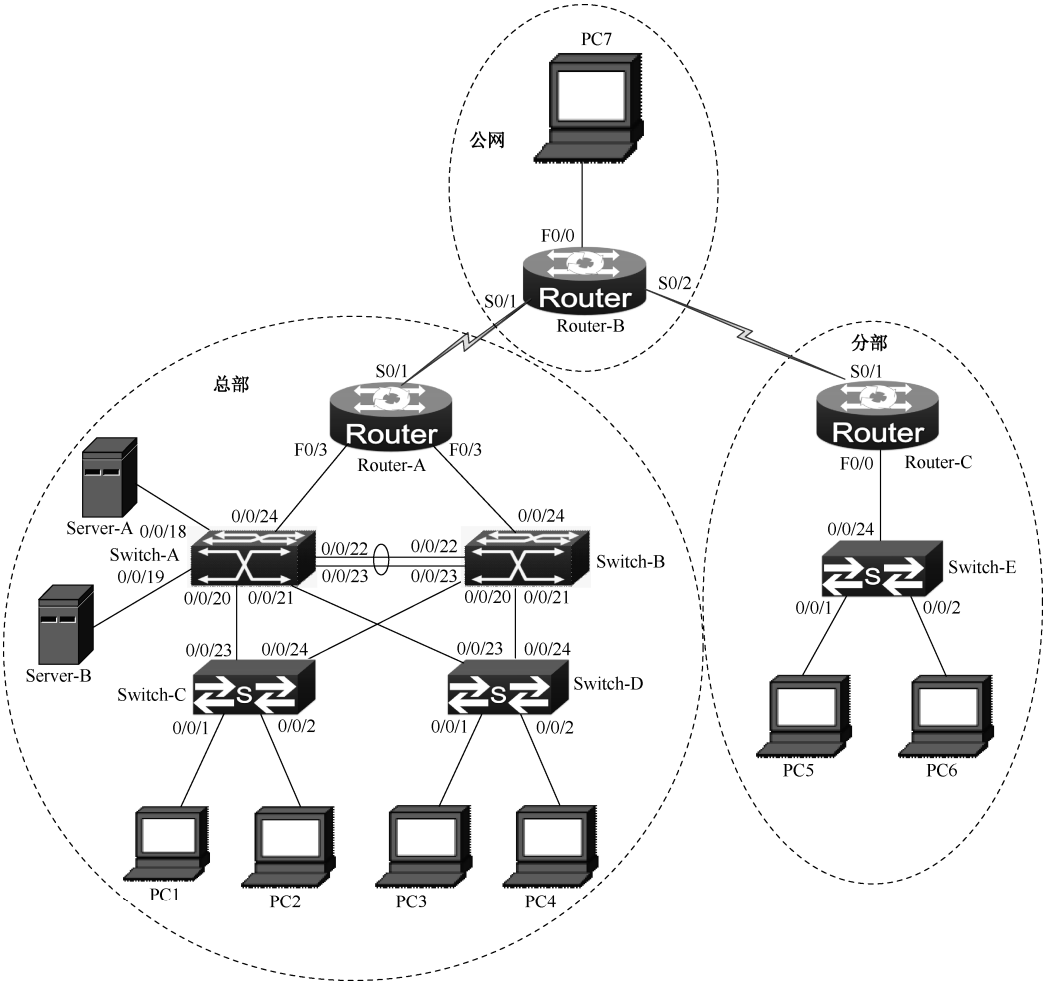


图 8-1-1　网络互连的拓扑结构

2. 地址规划

根据要求确定各接口的 IP 地址，见表 8-1-1。

表 8-1-1 IP 地址配置表

设　　备	设备型号	设备接口	IP 地址
Router-A	DCR-2626	Serial 0/1	140.10.1.5/30
		Ethernet 0/0	192.168.10.37/30
		Ethernet 0/3	192.168.10.41/30
Router-B	DCR-2626	Serial 0/1	140.10.1.6/30
		Serial 0/2	150.10.1.5/30
		Ethernet 0/0	160.10.1.5/24
Router-C	DCR-2626	Serial 0/1	150.10.1.6/30
		Ethernet 0/0.1	172.16.70.254/24
		Ethernet 0/0.2	172.16.80.254/24
Switch-A	DCRS-5650	Ethernet 0/1	192.168.10.38/30
		VLAN 100 SVI（服务器群）	192.168.10.65/27
		VLAN 10 SVI（销售部）	192.168.10.97/27
		VLAN 20 SVI（管理部）	192.168.10.129/27
		Port-channel 1（Port 22 和 23）	
Switch-B	DCRS-5650	Ethernet 0/1	192.168.10.42/30
		VLAN 10 SVI（销售部）	192.168.10.126/27
		VLAN 20 SVI（管理部）	192.168.10.158/27
		Port-channel 1（Port22 和 23）	
Switch-C	DCRS-5650	与 Switch-A 和 Switch-B 采用标准协议连接	划分 VLAN 10 和 20
Switch-D	DCRS-5650	与 Switch-A 和 Switch-B 采用标准协议连接	划分 VLAN 10 和 20
Switch-E	DCS-3950	与 Router-C 采用标准协议连接	划分 VLAN 70 和 80
Server-A		属于 VLAN 100	192.168.10.66/27
Server-B		属于 VLAN 100	192.168.10.67/27
PC-1		属于 VLAN 10	DHCP（Switch-B）获得 IP 网段
PC-2		属于 VLAN 20	
PC-3		属于 VLAN 10	
PC-4		属于 VLAN 20	
PC-5		属于 VLAN 70	DHCP（Router-B）获得 IP 网段
PC-6		属于 VLAN 80	
PC-7		与 Router-B 的以太口相连	160.10.1.6/24

3. 任务要求

（1）根据题中给出的拓扑结构图配置设备名称。

（2）在所有网络设备上为特权用户增加密码“ passworddcn ”，密码以加密方式存储。

（3）在各三层交换机和路由器上设置 Telnet 登录，登录用户名为 usertest，密码为 passwordtest，密码以明文方式存储，路由器中的登录验证方法名为系统默认名称，此方法

使用本地数据库验证，在路由器 Router-C 上为特权用户添加密码“ passenable ”，用户级别为最高级，密码以明文方式存储。

（4）在三层交换机 Switch-A 上划分各 VLAN，并加入相应的端口，见表 8-1-2。

表 8-1-2　Switch-A 的 VLAN 划分

VLAN	name	端　口　号
VLAN 100	Dept01	
VLAN 20	Dept02	
VLAN 100	Server	E0/0/18，E0/0/19
VLAN 110		E0/0/24

上表中未提到的端口放在 VLAN 1 中。

（5）在三层交换机 Switch-B 上划分各 VLAN，并加入相应的端口，见表 8-1-3。

表 8-1-3　Switch-B 的 VLAN 划分

VLAN	name	端　口　号
VLAN 10	Dept01	
VLAN 20	Dept02	
VLAN 100		E0/0/24

上表中未提到的端口放在 VLAN 1 中。

（6）在二层交换机 Switch-C 上划分各 VLAN，并加入相应的端口，见表 8-1-4。

表 8-1-4　Switch-C 的 VLAN 划分

VLAN	name	端　口　号
VLAN 10	Dept01	E0/0/1、E0/0/11-E0/0/13
VLAN 20	Dept02	E0/0/2、E0/0/14-E0/0/16

上表中未提到的端口放在 VLAN 1 中。

（7）在二层交换机 Switch-D 上划分各 VLAN，并加入相应的端口，见表 8-1-5。

表 8-1-5 Switch-D 的 VLAN 划分

VLAN	name	端　口　号
VLAN 10	Dept01	E0/0/1、E0/0/11-E0/0/13
VLAN 20	Dept02	E0/0/2、E0/0/14-E0/0/16

上表中未提到的端口放在 VLAN 1 中。

（8）根据拓扑结构图在各交换机上创建各 VLAN，给虚拟接口配置 IP 地址（VLAN1 为管理 VLAN）。

（9）在三层交换机 Switch-A 和 Switch-B 上配置路由冗余协议和多生成树协议，使总公司员工安全稳定地使用网络工作。

（10）在 Switch-B 上实现 DHCP 服务器，要求为 PC1、PC2、PC3 和 PC4 所在的子网提供自动分配 IP 地址服务，租期为 4 天。

（11）为 Switch-A 的端口 4 设定端口带宽限制，出入口均限速 1Mb/s。

（12）为 Switch-B 的端口 8 上配置广播风暴抑制，允许通过的广播包数为每秒 5000。

（13）根据拓扑结构图，将三台路由器的 Serial 口用背对背线缆连接，带宽为 2048000b/s，线缆连接时注意确保 Router-C 为 DTE 端，Router-B 为 DCE 端，速率为 2048000b/s。封装需要进行 CHAP 验证的 PPP，验证方法列表名为“ test ”；DCE 端的路由器用户名为“ userdce ”，密码为“ chappass ”；DTE 端的路由器用户名为“ userdte ”，密码为“ chappass ”，密码用明文显示。

（14）根据拓扑结构图在各路由器上相关位置配置 IP 地址，对快速以太网口添加描述明确的连接对象。

（15）总公司内部配置动态路由协议 RIPv2，分公司内部配置动态路由 RIPv2 使得全网连通，总公司、分公司与公网的外网之间使用 OSPF 路由协议，实现内部和外部网络的互相通信。

（16）在 Router-B 上实现 DHCP 服务器，要求为 PC5 和 PC6 所在的子网提供自动分配 IP 地址服务，租期为 4 天。

（17）在 Router-B 上实现单臂路由，使得 PC5 和 PC6 可以相互通信。

（18）路由器快速以太口速率为 100Mb/s，工作在全双工模式。

（19）上班时间禁止 PC1 所在网段访问 PC7 所在网段，ACL 名称为 worktime。

（20）在交换机 D 上实现 PC4 的 MAC 地址与 E0/0/2 端口的绑定，该端口的最大安全 MAC 地址数为 3，锁定该端口。

（21）配置 Switch-B，使其能够通过 Web 方式访问交换机，Web 授权用户为 admin，口令为加密的 adminpass。

（22）禁止 PC2 连通 PC6，但 PC6 可以连通 PC2。

（23）完成配置后将各设备的配置文件捕获成 TXT 格式，并保存。

步骤实现

详细配置请参见本书教学资源。

学习小结

本学习任务综合应用到了本书所学的二层交换机、三层交换机和路由器配置的基本知识，主要包括了交换机配置文件清空、交换机的几种配置模式、交换机命名、基于端口的 VLAN 划分、VLAN 接口的 IP 地址配置、特权密码、Telnet 登录交换机、链路聚合、生成树协议、虚拟网关路由协议，三层路由通信和路由器的命名、单臂路由、RIP、OSPF、广播风暴、PPP、VPN、DHCP、ACL 和 NAT 等知识。

学习任务 2　企业网络综合实战

学习情境

某公司由于公司业务规模的扩大，现分成了东区和西区，两个厂区相隔不远。东西两厂区之间准备通过路由器的 VPN 专线技术实现互连。东厂区作为公司互联网出口，东西两个厂区均通过该接口访问互联网。公司的主要服务器放在东厂区防火墙的 DMZ 中。在西厂区中使用两台三层交换机作为双核心，交换机设置链路聚合以提高交换机之间的带宽。另外，交换机之间还提供了一条线路作为备份链路，以备聚合链路出现故障时使用。西厂区各大楼划分 VLAN 管理。两厂区之间数据通过 VPN 实现加密传输。优化网络配置，使得整个公司网络高效、稳定、安全。公司需要搭建多种网络服务，提供主页发布、文件共享、邮件收发等常用功能。公司为方便会议使用网络和来访客人使用互联网，特意架设了无线网络。

情境分析

1. 网络连接

根据需求分析的描述与下列详细要求完成网络结构的设计与设备的连接，画出完整的网络拓扑结构图。拓扑结构图中需要明确列出设备接线的端口号，以及端口相关的 IP 地址。实际接线与设置必须按照拓扑结构图进行。

完成网络的规划设计后，请按以下要求进行网络的连接与配置。

（1）东厂区使用一台防火墙作为网络唯一出口接入互联网，PC1 模拟互联网上的计算机；Server 也接入该防火墙的 Eth0/1 作为公司网内服务器。

（2）Server 作为服务器主机。

（3）西厂区使用一台路由器与东厂区路由器通过 VPN（IPSec）技术互连；东厂区的路由器通过 F0/0 口与防火墙相连；西厂区的路由器分别下连两台三层交换机作为汇聚交换机，分别通过三层互连；两台三层汇聚交换机之间通过两条线路进行链路汇聚通信，另外一条线路作为链路备份，汇聚交换机下连一个接入层交换机。

（4）无线 AC 接在汇聚交换机上，并下连无线 AP，通过 AP 可以实现无线上网。

（5）PC1 和 PC2 接入二层交换机，PC1 和 PC2 的 IP 地址自动获取，服务器为 Switch-A。PC1 划归 VLAN10，PC2 划归 VLAN20。

（6）根据设计估算所需要的耗材数量，准备好领料清单。

（7）根据上述要求完成拓扑设计后，制作线缆完成设备的连接。

（8）打配的跳线使用 T568B 线序，制作的线缆必须稳固耐用。

根据要求画出公司的网络拓扑结构图，如图 8-2-1 所示。

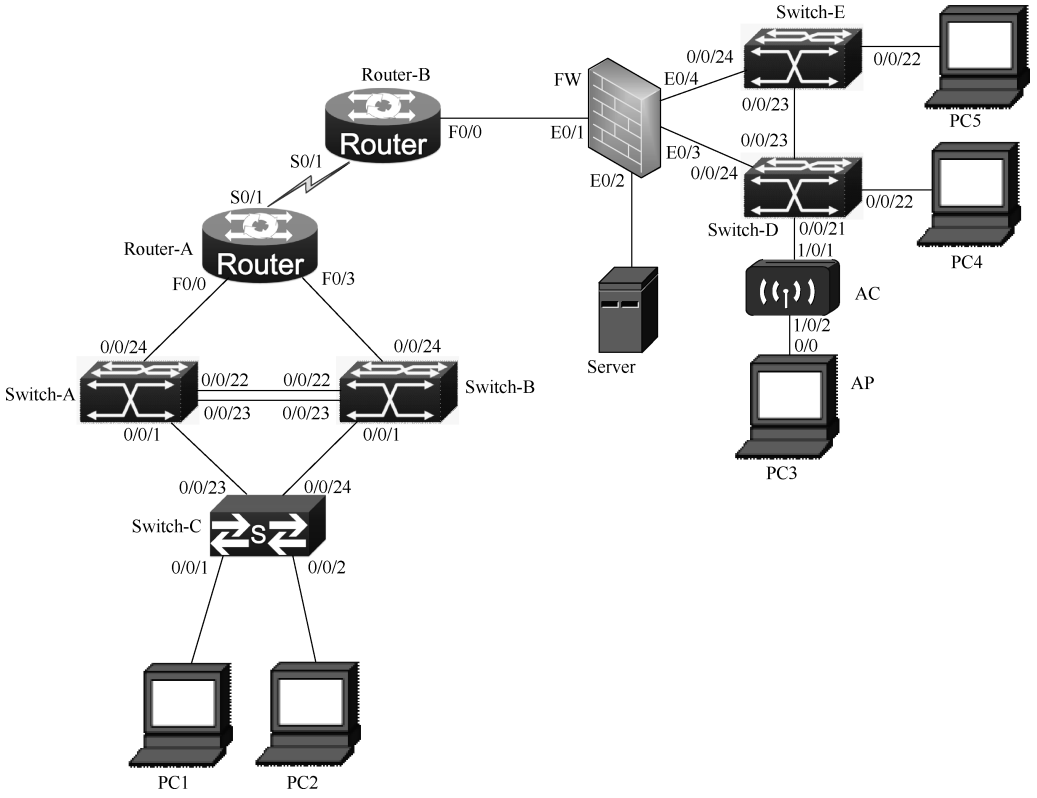


图 8-2-1　公司网络拓扑结构

小贴士

（1）画图时应标出各设备名称、所连端口号。

（2）PC 和路由器相连、交换机和交换机相连必须用交叉线。

（3）线路连接好之后应检查指示灯是否工作正常。

2. 网络地址划分

(1)路由器 A 的 S0/1 端口地址为 172.16.1.1/30, 路由器 B 的 S0/1 端口地址为 172.16.1.2/30, 作为社区间互连地址。

（2）东厂区使用 172.16.2.0/24 作为内部网络地址段，其中以最后一个有效 IP 地址作为网关，Server 主机使用第一个有效 IP 作为地址。

（3）东厂区路由器的防火墙接入互联网地址为 10.10.10.1/30。PC4 和 PC5 作为东厂区内网中的机器。

（4）东厂区路由器 F0/0 端口地址为 172.16.1.5/30；东厂区防火墙 E0/0 端口地址为 172.16.1.6/30。

（5）西厂区有两栋办公楼，每栋办公楼有 40～50 个用户。请使用 192.168.1.0/24 网段进行子网规划，划分两个 VLAN，分别为 VLAN10 和 VLAN20。VLAN10 是用 192.168.1.0/24 网段子网划分后的第一个有效子网。VLAN20 是用 192.168.1.0/24 网段子网划分后的第二个有效子网，使得每栋楼都有一个独立的网段，每个网段的网关使用该网段最后一个有效的网

络地址。

（6）二层交换机 A 的 1、3～10 号端口划归 VLAN10；2、11～19 号端口划归 VLAN20，根据子网规划，在网络设备中设定 VLAN。

（7）交换机的端口地址（各子网网关的端口地址根据要求设定）。

交换机 A 端口 24 指定网关路由地址为 192.168.2.1/24。

交换机 B 端口 24 指定网关路由地址为 192.168.3.1/24。

（8）路由器 A 以太网端口地址端口 0/0 地址为 192.168.2.2/24、端口 0/3 地址为 192.168.3.2/24。

根据要求确定各接口 IP 地址，见表 8-2-1。

表 8-2-1 IP 地址配置表

设　备	端　口	IP 地址	网　关
Router-A	S0/1	172.16.1.1/30	无
Router-A	F0/0	192.168.2.2/24	无
Router-A	F0/3	192.168.3.2/24	无
Router-B	F0/0	172.16.1.5/30	无
Router-B	S0/1	172.16.1.2/30	无
Switch-A	E0/0/24	192.168.2.1/24	无
Switch-A	VLAN10	192.168.1.125/26	无
Switch-A	VLAN20	192.168.1.189/26	无
Switch-B	E0/0/24	192.168.3.1/24	无
Switch-B	VLAN10	192.168.1.126/26	无
Switch-B	VLAN20	192.168.1.190/26	无
Switch-C	VLAN10	无	无
Switch-C	VLAN20	无	无
Switch-D	E0/0/24	10.10.10.2/30	
Switch-D	VLAN10	10.10.10.9/30	
Switch-E	E0/0/24	10.10.10.6/30	
Switch-E	VLAN20	10.10.10.13/30	
Server		172.16.2.1/24	172.16.2.254
FW	E0/1	172.16.1.6/30	
FW	E0/2	172.16.2.254/24	
FW	E0/3	10.10.10.1/30	
FW	E0/4	10.10.10.5/30	
PC1	E0/0/1	自动获取	自动获取
PC2	E0/0/2	自动获取	自动获取
PC3	无线连接	自动获取	自动获取
PC4	E0/0/22	10.10.10.10/30	10.10.10.9/30
PC5	E0/0/22	10.10.10.14/30	10.10.10.13/30

小贴士

（1）划分子网时应看清楚要求。

（2）数制转换应细心，转换后一定要对转换的结果进行检验。

（3）IP 地址的使用以尽量节约为原则。

3. 任务要求

所需设备：

（1）DCRS-5650 交换机 2 台。

（2）DCS-3950 交换机 1 台。

（3）DCR-2626 路由器 2 台。

（4）DCFW-1800 防火墙 1 台。

（5）DCWS-6028 无线 AC1 台。

（6）DCWL-7962AP 1 台。

（7）PC 4 台。

（8）带无线网卡的笔记本式计算机 1 台。

（9）Console 线 3 条。

（10）CR-V35MT 1 条。

（11）CR-V35FC 1 条。

具体要求如下：

（1）设定各设备的名称，格式如下：交换机命名为“ Switch-A ”、“ Switch-B ”、“ Switch-C ”、“ Switch-D ”和“ Switch-E ”；路由器命名为“ Router-A ”和“ Router-B ”，防火墙命名为“ FW ”，无线控制器命名为“ AC ”，无线接入点命名为“ AP ”。

（2）Router-A 设置 Telnet 登录，登录用户名为 Teluser，密码为 admin。

（3）为 5 台交换机的特权用户增加密码 super123，密码以加密方式存储。

（4）手动配置三层交换机通过 22、23 端口实现链路聚合。

（5）在交换机上开启生成树协议。

（6）在 Switch-A 和 Switch-B 上实现 VRRP 协议，Switch-A 为 master。

（7）在 Switch-A 上实现 DHCP 协议，使得 PC1 和 PC2 自动获取地址等信息。

（8）为 Switch-A 的端口 4 设定端口带宽限制，出入口均限速 1Mb/s。

（9）在 Switch-B 的端口 8 上配置广播风暴抑制，允许通过的广播包数为每秒 5000。

（10）配置串口二层链路为 PPP 封装模式，采用 CHAP 认证方式实现双向认证，Router-A 上的用户名为 userB，密码为 shenzhou；Router-B 上的用户名为 userA，密码为 shenzhou。

（11）西厂区的内部网络使用 RIP 路由协议，东厂区的内部网络利用 OSPF 路由协议，最终实现东西厂区之间的网络互连。

（12）配置 Router-A，禁止 VLAN20 访问互联网。

（13）在 Router-A 和 Router-B 上分别配置建立 VPN 通道，要求使用 IPSec 协议的 ISAKMP 策略算法保护数据，配置预共享密钥，建立 IPSec 隧道的报文使用 MD5 加密，IPSec 变换集合定义为“ ah-md5-hmas　esp-3des ”。两台路由器串口互连，Router-A 作为 DCE 端。

（14）为保证内部网络安全，防止互联网的机器窥探内部网络，利用防火墙隐藏内部网络地址使得外网用户不能直接访问园区网内的机器。

（15）通过配置防火墙内部地址能通过网络地址转换方式访问互联网。

（16）在防火墙中使用合法 IP 地址 1.1.1.1 为 Server 配置 IP 映射，允许内外网用户通过外网 IP 实现对该 Server 的 Web 访问。

（17）震荡波病毒常用的协议端口为 TCP 协议 5544 和 445，请配置三层交换机以防止病毒在局域网内肆虐。

（18）PC2 中已经搭建好了 TFTP 服务。将所有网络设备的配置文件通过 TFTP 服务备份到 PC2 的 TFTP 服务器根目录中。

（19）通过对 AC 的适当配置，使得 AP 可以在公司没有有线网络的位置能使用无线上网。

步骤实现

详细配置请参见教学资源。

学习小结

本任务综合应用到了本书所学的安全知识，包括计算机的安全接入、通过访问控制列表实现访问控制、设置网络设备权限、路由器的安全连接以及网线制作等知识，所以必须熟练掌握这些知识点。通过本项目的训练，将进一步提高动手能力和综合素质。

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传　　真：（010）88254397

E-mail：　dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

　　电子工业出版社总编办公室

邮　　编：100036